FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

# Zadání bakalářské práce

| | |
|---|---|
| **Název:** | Monitorování nechtěného sledování uživatelů mobilními telefony na platformě Android |
| **Student:** | Patrik Suchopa |
| **Vedoucí:** | Ing. Jan Fesl, Ph.D. |
| **Studijní program:** | Informatika |
| **Obor / specializace:** | Bezpečnost a informační technologie |
| **Katedra:** | Katedra počítačových systémů |
| **Platnost zadání:** | do konce letního semestru 2022/2023 |

## Pokyny pro vypracování

V rámci bakalářské práce se zaměřte na ověření hypotézy a sice, že "mobilní telefony s operačním systémem Android mohou být zneužity pro sledování uživatelů bez jejich vědomí". Sledování uživatelů může probíhat různými způsoby jako např. reportováním jejich GPS polohy, skenováním dostupných Wi-Fi sítí, zasíláním osobních informací nebo rozpoznáváním hlasového projevu uživatele. Všechny tyto typy sledování (popř. i další) důkladně prozkoumejte, navrhněte a implementujte jejich detekci. Pokud nebude možné některý typ sledování spolehlivě detekovat, řádně vysvětlete technickou podstatu problému.

Detekce škodlivé aktivity proveďte ve dvou rovinách: z pohledu kontinuálního sledování síťového provozu (primárně) a z pohledu změn ve využití systémových prostředků (sekundárně). Postupujte inkrementálním způsobem, tj. nejprve prozkoumejte mobilní telefon s čerstvě nainstalovaným operačním systémem a následně prozkoumejte předem vytipované potenciálně škodlivé aplikace.

---

*Elektronicky schválil/a prof. Ing. Pavel Tvrdík, CSc. dne 20. července 2021 v Praze.*

Bakalářská práce

# MONITOROVÁNÍ NECHTĚNÉHO SLEDOVÁNÍ UŽIVATELŮ MOBILNÍMI TELEFONY NA PLATFORMĚ ANDROID

**Patrik Suchopa**

Fakulta informačních technologií
Katedra počítačových systémů
Vedoucí: Ing. Jan Fesl, Ph.D.
11. května 2022

# Obsah

# Seznam obrázků

# Seznam tabulek

*Chtěl bych poděkovat především Ing. Janu Feslovi, Ph.D. za vedení bakalářské práce, jeho rady a čas strávený na konzultacích. Děkuji také své rodině za vytvoření perfektních podmínek při průběhu studia.*

# Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů, zejména skutečnost, že České vysoké učení technické v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 citovaného zákona.

V Praze dne 11. května 2022 .....

# Abstrakt

V bakalářské práci se věnuji návrhům a implementaci způsobů detekce nechtěného sledování uživatelů mobilními telefony na platformě Android. K tomuto účelu jsou analyzována data získaná monitorováním síťového provozu mobilního telefonu i změn ve využití procesoru a operační paměti. Výsledkem práce je aplikace pro datovou analýzu. Měřením nebyl detekován odposlech uživatelů, nepodařilo se prokázat aktivitu spojenou se zpřesňováním zeměpisné polohy využitím okolních Wi-Fi sítí. Byla detekována neočekávaná aktivita spojená s aplikací Mapy Google, kdy probíhala komunikace s jejími doménami i přesto, že byla aplikace formálně vypnutá.

**Klíčová slova** operační systém Android, mobilní telefon, sledování uživatelů, soukromí uživatelů, sledování síťového provozu, využití systémových prostředků, wireshark

# Abstract

This bachelor thesis deals with the design and implementation of detection methods related to unwanted monitoring of users by mobile phones on the Android platform. Monitoring network traffic and usage of system resources gave me data subjected to analysis. I implemented the application designated for data mining beyond requirements. I could not detect eavesdropping of users nor activity allied with improving users' localization by Wi-Fi scanning. There was an unexpected behavior related to the Google Maps application. The communication with its domains occurred even though the application was terminated.

**Keywords** operating system Android, mobile phone, user tracking, user privacy, network traffic monitoring, usage of system resources, wireshark

# Seznam zkratek

| | |
|---|---|
| ADB | Android Debug Bridge |
| AP | Access Point |
| API | Application Programming Interface |
| ART | Android Runtime |
| B | Bajt |
| CPU | Central Processing Unit |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Domain Name System |
| GB | Gigabajt |
| GHz | Gigahertz |
| GPS | Global Positioning System |
| HAL | Hardware Abstraction Layer |
| ICMP | Internet Control Message Protocol |
| IP | Internet Protocol |
| KB | Kilobajt |
| MB | Megabajt |
| NAT | Network Address Translation |
| OS | Operační systém |
| RAM | Random Access Memory |
| SIM | Subscriber Identity/Identification Module |
| SMS | Short Message Service |
| SNIe | Server Name Indication extension |
| TCP | Transmission Control Protocol |
| TLS | Transport Layer Security |
| UDP | User Datagram Protocol |
| USB | Universal Serial Bus |

# Úvod

Mobilní telefony tvoří nedílnou součást našich životů. Vývoj aplikací se řídí stále větší poptávkou po co největší integraci každodenních životů do těchto zařízení. Jejich hlavní účel už dnes není jen a pouze zprostředkování hovorů, ale už slouží kupříkladu jako GPS navigace nebo hlasový asistent. S tímto ovšem vyvstává i otázka práce s osobními údaji. Ty se staly na trhu velmi žádanou komoditou, vývojáři aplikací jich sbírají nepřeberné množství často za jediným účelem – větším přizpůsobením aplikací uživatelům. Pod přizpůsobením si lze představit dnes běžný návrh videí ke shlédnutí na základě předchozí aktivity nebo reklamy na míru, třeba dle zaznamenané zeměpisné polohy. Ovšem jak ukázaly události posledních let, ne vždy se data sbírají se souhlasem uživatelů nebo tak, jak autoři aplikací tvrdí. V horších případech se osobní informace stávají prostředkem utajovaných obchodů. Téma sběru a následné práce s osobními údaji se tak stalo frekventovaným celospolečenským tématem. Práce se proto věnuje detekci nežádoucího sledování uživatelů prostřednictvím mobilních telefonů na platformě Android.

Někteří uživatelé mobilních telefonů na zmíněné platformě mohli nabýt dojmu, že o nich aplikace nebo obecněji mobilní telefony sbírají více informací, než ke svým deklarovaným účelům potřebují. Práce je proto určena zejména těmto uživatelům. Práce může ovšem posloužit také k poskytnutí základní představy o tom, jak může být sběr osobních údajů řešen (nejen) aplikacemi na jiných platformách. Jelikož se dá předpokládat, že tam mohou být jisté podobnosti.

Motivací pro výběr tohoto tématu byl výskyt neočekávaného přizpůsobení nabízených reklam v mém okolí, patrně jako důsledek odposlechů bez vědomí a souhlasu těchto uživatelů.

Cílem práce je navrhnout a implementovat způsob detekce z hlediska kontinuálního sledování síťového provozu i z pohledu změn využití systémových prostředků mobilního telefonu.

V teoretické části práce se věnuji historii mobilních telefonů, představuji jejich senzory a princip systémových oprávnění, přičemž na zaznamenaných událostech dokazuji jejich potenciální zneužitelnost. Dále se věnuji historii operačního systému Android a popisu jeho architektury.

Praktická část práce se věnuje popisu vybraných nástrojů využitých během tvorby bakalářské práce. Dále popisuji návrh počítačové sítě, na jejímž základě bude odposlouchávána síťová komunikace mobilního telefonu a zároveň budou zaznamenávány informace o změnách ve využití systémových prostředků telefonu. Následně popisuji scénáře a vlastnosti jednotlivých měření i analýzu získaných dat, která bude využita na závěr jako podklad pro vyhodnocení hypotézy „Mobilní telefony s operačním systémem Android mohou být zneužity pro sledování uživatelů bez jejich vědomí.“

# Kapitola 1
# Cíl práce

Hlavním cílem práce je ověřit, zda může docházet ke sledování uživatelů skrze mobilní telefony na platformě Android bez jejich souhlasu nebo vědomí. Sledováními, která budou v práci zkoumána se rozumí reportování GPS polohy, rozpoznávání hlasového projevu a skenování dostupných Wi-Fi sítí. V práci se věnuji návrhu a implementaci počítačové sítě, na níž bude odposlouchávána komunikace mobilního telefonu a zároveň zaznamenáváno využití systémových prostředků. Detekce bude postupovat inkrementálním způsobem, tedy nejprve na telefonu v továrním nastavení a poté s vytipovanými potenciálně škodlivými aplikacemi. Sesbíraná data budou poté předmětem analýzy, jíž závěry budou využity při vyhodnocení hypotézy „Mobilní telefony s operačním systémem Android mohou být zneužity pro sledování uživatelů bez jejich vědomí.“

# Kapitola 2
# Sledování uživatelů

V této kapitole se věnuji stručnému popisu vývoje existence mobilních telefonů. Dále popisuji senzory mobilních telefonů, základní princip systémových oprávnění, přičemž u těchto oblastí také různými zjištěními dokazuji jejich možnou zneužitelnost. Zároveň zde také zmiňuji publikace svým zaměřením nebo způsobem řešení podobné této bakalářské práci.

## 2.1 Mobilní telefony

Psal se rok 1973, když se uskutečnil první hovor prostřednictvím mobilního telefonu. Tehdejší pracovník společnosti Motorola, Martin Cooper, se rozhodl zavolat do konkurenční společnosti, aby je informoval, že s nimi právě přes jeden hovoří [1]. Mobilní telefony byly pouze na počátku svého vývoje, takže ani ony ani zařízení jim podobná nebyly zpočátku dostupné široké veřejnosti, nýbrž vývojářům, případně významnějším (movitějším) institucím. Starostí spojených s jejich využíváním, zejména z pohledu bezpečnosti, proto nebylo mnoho. Možná až na poskytnutí bazálního zabezpečení za účelem zamezení, nebo přinejmenším ztížení odposlechu dokonce téměř nulová.

Jak plynul čas, nezaostával ani technologický vývoj a přirozeně stále zrychlující evolucí procházel také návrh a vývoj mobilních telefonů. Mobilní telefony se postupně zmenšovaly, jejich samotná výroba nebyla tak monopolizována, což v důsledku vedlo k razantnímu snížení ceny a tím i zvýšení dostupnosti. Důkazem široké dostupnosti budiž fakt, že k lednu 2022 bylo na světě 5,31 miliard unikátních uživatelů mobilních telefonů, což činilo přibližně 67 % světové populace [2]. Lidé tak vzali mobilní telefony za své, začlenili je do svých životů natolik, až si bez nich mnozí už svůj osobní nebo profesní život nedokáží představit. Prakticky permanentní přístup k mobilním telefonu ale znamená přítomnost mnohem většího počtu potenciálních rizik, než v 70. letech 20. století.

## 2.2 Senzory

Senzory v zařízeních na platformě Android je možno rozdělit do 4 kategorií:

- lokalizační (GPS…),
- grafické (fotoaparát, kamera…),
- zvukové (mikrofon…),
- standardní (gyroskop, akcelerometr…).

Senzory spadající do těchto kategorií dokáží sbírat poměrně širokou škálu uživatelských dat, od obrazových dat pomocí fotoaparátu, přes zeměpisnou polohu udávanou GPS senzorem, až po mluvené slovo uživatele prostřednictvím mikrofonu. Ačkoli senzory dokáží sbírat potenciálně velmi dobře zneužitelné údaje, neexistoval žádný propracovaný systém zaznamenávající přístup k senzorům. Ten by případně mohl zaznamenat přístup k datům z třetích stran. Vzorek čítající bezmála 1500 nejpopulárnějších Android aplikací (původem ze tří různých obchodů) ukázal, že více než čtvrtina přistupuje k senzorům při spuštění aplikace a 11 % z nich i přesto, že běží pouze na pozadí [3].

### 2.2.1 Lokalizační senzory

Dovolte mi z hlediska sledování uživatelů vyzdvihnout lokalizační senzory. Ty jsou dnes skrze GPS, případně podobné systémy, běžnou součástí mobilních telefonů, nezávisle na platformě. Tyto senzory dokáží s relativně vysokou přesností určit zeměpisné souřadnice libovolného bodu, neboli mobilního telefonu a tudíž samotného uživatele. Lze předpokládat, že nejčastější *vědomé* využití této funkcionality je způsobeno mapovými aplikacemi. Co se sledování týče, v případě přesunu z bodu A do bodu B je snímání uživatelské polohy v reálném čase jistě žádoucí – pokud mu skutečně předcházelo rozhodnutí o využití aplikace při pohybu. Nicméně to, že uživatel souhlasí s tím, aby jeho lokalizační údaje zpracovávala jistá aplikace ještě neznamená, že chce, aby byly volně dostupné ostatním lidem nebo aplikacím. Proto se nabízí šifrování jako efektivní nástroj ochrany dat. Ovšem jak ukazuje [4], někteří vývojáři takové údaje vkládali do aplikace Mapy Google v nezašifrované podobě, a to i přes doporučení jejich autorů.

Explicitní lokalizační údaje, ale nejsou jedinou možností, jak determinovat uživatelovy souřadnice, jelikož toho lze docílit také skenováním okolních Wi-Fi sítí. Poskytovatelé lokalizačních služeb si totiž uchovávají databázi, naplněnou co největším množstvím informací o přístupových bodech (Access Points, AP) bezdrátových sítí. Z toho vyplývá, že je možné skenovat okolí uživatele, speciálně jemu dostupné Wi-Fi sítě, načež propojením s údaji jednotlivých AP lze určit uživatelovu „cestovatelskou historii“ až s přesností přesahující 90 % [5].

### 2.2.2 Zvukové senzory

Některé organizace vyvíjí vlastní hlasové asistenty, kteří umožňují ovládat zařízení (telefon) pomocí hlasu. V principu fungují tak, že jsou pasivní většinu času a aktivně komunikovat s uživatelem začnou až ve chvíli, kdy jsou „probuzení“ vyslovením nějaké hlášky, kupříkladu „Ok, Google“. V roce 2019 reportéři veřejnoprávní VRT NWS z Nizozemí přišli s informací, že zaměstnanci Google poslouchají hlasové záznamy uživatelů. Podle oficiálního vyjádření Google se jedná pouze o 0,2 % všech záznamů, přičemž dodává, že tak koná za účelem zlepšení Google asistenta. Navíc prohlásil, že zmíněné záznamy neobsahují žádnou informaci, díky které by bylo možné uživatele jednoznačně identifikovat [6].

Hlasový odposlech však může probíhat i jinak, například využitím mikrofonu. Až do verze Android 9.0 (Pie) bylo možné, aby aplikace běžící na pozadí získala přístup k mikrofonu a tedy nahrávala zvuk bez uživatelova vědomí. Pravděpodobně se jednalo o chybu v návrhu, poněvadž později byla tato možnost odstraněna [7].

## 2.3 Systémová oprávnění

Systémová oprávnění aplikací v telefonu jsou dalším faktorem ochrany dat. Oprávnění ve vší obecnosti slouží k omezení přístupu různým entitám (lidem, aplikacím…). V případě zeměpisných souřadnic může být cílem zajistit, aby k nim nebo k jejich určení zdaleka ne všechny aplikace měly přístup. Avšak [8] popisuje, jak Google aplikace MyTracks umožňovala zaslat tyto údaje aplikacím, které k nim na základě oprávnění neměly mít přístup.

Ovšem nemusí jít jen o nedůsledné dodržování či dokonce vědomé ignorování těchto nastavení. Způsob fungování oficiálního obchodu s aplikacemi pro platformu Android – Obchod Play – klade nemalou míru zodpovědnosti na bedra uživatelů. Před stažením aplikace si lze prohlédnout oprávnění, která aplikace pro svou funkčnost vyžaduje. V případě, že si uživatel vyhodnotí už v tomto kroku aplikaci jako nežádoucí (například kvůli výskytu pro danou aplikaci neočekávaných oprávnění) a následně odmítne její instalaci, může předejít potenciálním nepříjemnostem. Nicméně [9] ukazuje, že jen zhruba 20 % uživatelů dělá starost chování mobilních aplikací vůči jejich soukromí.

## 2.4 Podobná práce

Cílem několika výzkumů bylo skutečné chování aplikací z hlediska přístupu k citlivým osobním údajům uživatele. Výzkum ústící ve vývoj aplikace PrivacyMod zkoumá některé operace prováděné aplikacemi. Za zmínku stojí přístup k zeměpisným souřadnicím, SMS zprávám nebo kontaktům. Mezi nejzajímavější zjištění se po mém soudu řadil fakt, že vypnutá aplikace Twitter přistupovala k lokalizačnímu Google API (Application Programming Interface). Tomu následuje i zjištění, že aplikace si při instalaci řeknou o „větší“ oprávnění, než fakticky využívají [10].

Dále bylo zjištěno, že aplikace Počasí opakovaně přistupovala ke kontaktům v telefonu, což není očekávaná vlastnost takové aplikace [11]. Ovšem je fér říci, že od těchto výsledků uplynulo 7 let, což je poměrně dlouhá doba a od té doby se situace mohla výrazným způsobem změnit.

# Kapitola 3
# Operační systém Android

Tato kapitola se věnuje popisu operačního systému Android, jeho historii, využívanosti i popisu architektury celého operačního systému.

## 3.1 Historie

Vznik operačního systému Android se datuje do října roku 2003. Toho času zbývaly ještě 4 roky, než Steve Jobs na jedné z Apple konferencí představil mobilní telefon (smartphone) v principu takový, jak jej známe dnes. Ambicí autorů operačního systému Android bylo vyvinout chytřejší mobilní zařízení, která budou více vnímat uživatelovy osobní preference, či lokaci v níž se nachází. Avšak tomu předcházela snaha o vybudování nového operačního systému digitálních fotoaparátů. Kvůli nepřízni trhu museli autoři od tohoto záměru upustit, tudíž se zaměřili na mobilní telefony.

Psal se rok 2005, když si firmu Android Inc vyhodnotil jako výhodnou akvizici Google. Původní autoři se nedlouho poté podíleli na rozhodnutí vyvíjet operační systém na bázi jádra operačního systému Linux, jehož zdrojové kódy jsou veřejné. Tato volba umožnila poskytovat operační systém třetím stranám zdarma, přičemž byl předpoklad, že zisk dokáže generovat poskytování aplikací a jiných služeb. To se nakonec ukázalo jako vhodný model podnikání.

Zhruba měsíc poté, co Steve Jobs představil světu iPhone, přišel Google s vůbec první verzí Android, která byla určena pro veřejnost. Nebo alespoň přiznaná, protože až do tohoto momentu byl vývoj před veřejností skrýván. Pro vývojáře byl tedy odtajněn Android 1.0 beta. První mobilní telefony s tímto operačním systémem byly v prodeji na podzim roku 2008. Od té doby se operační systém Android etabloval na trhu s mobilními telefony, až na něm v lednu roku 2022 disponoval téměř 70% majoritou [12].

## 3.2 Architektura

Operační systém Android se skládá z několika logických celků, představím je od nejnižší úrovně.

**Jádro operačního systému Linux** Jak již bylo zmíněno, celý operační systém stojí na jádře operačního systému (OS) Linux. To se stará o komunikaci s hardwarovými součástmi zařízení pomocí ovladačů nebo o funkcionality z ještě nižší úrovně, kupříkladu o správu paměti.

**Hardware Abstraction Layer** HAL představuje úroveň abstrakce, jelikož se jedná o sadu knihoven, které zprostředkovávají přístup k hardwarovým součástem (fotoaparátu, senzorům…) v hierarchii architektury výše postaveným logickým celkům.[13]

**Android Runtime** ART je virtuální stroj, který poskytuje běhové prostředí systémovým aplikacím. Od verze 5.0 nahradil virtuální stroj Dalvik, který fungoval tak, že kompiloval (převáděl do strojového kódu) bajt kód (kód na vyšší úrovni než strojový kód, avšak na nižší než zdrojový kód, vychází ze zdrojového kódu) aplikace těsně před spuštěním. Taková kompilace se nazývá Just-in-time. Dalvik vznikal v době, kdy kapacita operační paměti v zařízeních dosahovala řádově nižších hodnot než dnes. Hlavní charakteristikou Just-in-time kompilace tedy byla šetrnost k dostupné operační paměti, nicméně se zvyšující se kapacitou vyplouvaly na povrch limity týkající se efektivního využití celé paměti. Proto ART podporuje Ahead-of-time kompilaci, kdy se zdrojový kód kompiluje mnohem dříve, než dojde k samotnému spuštění aplikace, například při instalaci [13, 14].

**Nativní knihovny** Tento modul je v hierarchii na stejné úrovni jako ART a obsahuje knihovny psané v jazycích C nebo C++. Tyto knihovny využívají některé části již zmíněných modulů, případně jsou skrze API Java framework zpřístupněny i mobilním aplikacím.

**Java API Framework** Jedná se o sadu funkcí, které zjednodušují přístup k funkcionalitám jádra operačního systému případně jiných modulů. Využívají se zejména při vývoji aplikací.

**Systémové aplikace** Na vrcholu celé architektury stojí aplikace, ať už systémové, či uživatelem (vývojáři) nainstalované [13].

# Kapitola 4
# Použité nástroje

Tato kapitola se věnuje popisu nejvýznamnějších hardwarových i softwarových nástrojů, jejichž záměrem bylo využít je během tvorby bakalářské práce.

## 4.1 Wireshark

Wireshark je open-source aplikace (vyvíjena s otevřeným zdrojovým kódem) disponující grafickým uživatelským rozhraním, sloužící k analýze provozu v počítačových sítích. Nástroj také nabízí možnost filtrování paketů (jednotek přenášených dat v síti), extrakci zvolené množiny dat nebo zobrazení jejich obsahu. Existuje více účelů užití nástroje Wireshark. Mezi nejčastější se může řadit průzkum komunikace síťového segmentu, například s využitím dříve zmíněných filtrů. Dále jej lze využít ve snaze o pochopení principů konkrétních komunikačních protokolů (sad pravidel pro komunikaci mezi zařízeními v síti) nebo v sítích vhodných rozměrů i k identifikaci chyb v jejich konfiguraci nebo implementaci.

## 4.2 Android Debug Bridge

Android Debug Bridge (ADB) je nástroj s textovým uživatelským rozhraním, jehož hlavní účel je ladění chyb v mobilních telefonech na platformě Android. Tím usnadňuje vývoj či instalaci aplikací, ale také umožňuje využít Unix shell (interpret příkazů z příkazové řádky), přes který je možno spouštět různé příkazy [15]. Jedním z příkazů, které shell akceptuje je dumpsys, jenž zprostředkovává přístup k diagnostickým informacím systémových služeb [16]. Některé z těchto informací dokáží poskytnout příkazy meminfo nebo cpuinfo. Ty konkrétně vypisují informace o momentálním stavu mobilního telefonu z hlediska využití operační paměti, respektive procesoru, jakož i o využití těchto prostředků konkrétními procesy nebo službami. Specifikum nástroje cpuinfo spočívá v tom, že spotřeba se udává v %, kde celkový součet může přesáhnout 100 %, jelikož je počítáno 100 % za každé fyzické jádro procesoru. Aktivace nástroje ADB je možná aktivací režimu vývojáře v mobilním telefonu, připojením telefonu přes kabel s koncovým USB (Universal Serial Bus) portem a následnému povolení přenosu souborů přes USB.

## 4.3 Bash

Bash je shell postavený na OS Unix, který tedy dokáže interpretovat příkazy z příkazové řádky. Díky němu lze například poměrně efektivně zpracovávat jednoduché textové soubory s neměnnou strukturou, což je případ výstupů příkazů meminfo a cpuinfo.

## 4.4 Python

Je nezbytné nad naměřenými daty provádět i komplexnější operace, ke kterým nejsou příkazy, které podporuje Bash vhodné. Pro tyto účely je vhodný programovací jazyk Python, jelikož je široce podporovaný a také jej doplňuje mnoho knihoven zaměřených na práci s daty. K tomuto účelu byly díky svým jednoduchým rozhraním zvoleny knihovny pandas a NumPy. K vizualizaci výsledků v podobě grafů jsem zvolil knihovnu Plotly, jejíž ne zcela efektivní implementaci vynahrazuje interaktivita při manipulaci s vykreslenými daty. Pro přívětivější práci s diagramy a pohodlnější filtrování vykreslených dat byla vytvořena jednoduchá grafická webová aplikace pomocí knihovny Streamlit, poněvadž je přímo určena k tomuto účelu [17]. Pro přívětivější konfigurování aplikace při spouštění z příkazové řádky byla využita i knihovna click. Všechny zmíněné knihovny mají také jeden společný rys a to ten, že jsou vyvíjeny veřejnou komunitou a tedy, že zdrojové kódy jsou volně přístupné.

## 4.5 Telefon

Subjektem měření byl mobilní telefon Alcatel 1B 2020, verze s 32 GB dostupné paměti. Na telefonu je nainstalován čistý operační systém Android 10 (Go Edition).

## 4.6 pmacct

Jedná se o open-source nástroj sdružující skupinu pasivních síťových monitorovacích nástrojů, jakými jsou například pmacctd, nfacctd a další. Tyto nástroje slouží k shromažďování dat síťového provozu, avšak na rozdíl od nástroje Wireshark neumožňují přístup k celým paketům, ale pouze k informacím typu zdrojová nebo cílová IP (Internet Protocol) adresa, použitý komunikační protokol a další [18].

## 4.7 MikroTik

Při několika měřeních byl využit router MikroTik RouterBOARD. Ten umožnil vygenerování řádově stovek rozdílných Wi-Fi sítí.

# Kapitola 5
# Návrh počítačové sítě

Tato kapitola představuje principy konfigurace běžné domácí sítě malých rozměrů. Dále popisuje i mou konkrétní situaci a možnosti segmentu sítě, k němuž mám přístup. Jelikož se nacházím v, po mém soudu, neobvyklých podmínkách, jsou zde dále popsány a okomentovány dvě řešení. První z nich se ukáže jako nevyhovující, proto jde zde navrženo a popsáno i druhé.

## 5.1 Popis situace

Z hlediska přenosového média existují dvě řešení, drátové a bezdrátové (Wi-Fi). Z pravidla se od počítačové sítě vyžaduje i přístup do Internetu. Obvyklý přístup v běžných domácích sítích malých rozměrů spočívá v konfiguraci routeru (směrovače), který bude sloužit jako brána mezi jednotlivými sítěmi, v tomto případě mezi malou lokální sítí a Internetem. Nová zařízení se poté do sítě připojují pomocí kabelu vedoucího přímo do routeru nebo i bezdrátové prostřednictvím Wi-Fi sítě. V případě, kdy je na routeru v provozu služba DHCP (Dynamic Host Configuration Protocol), která přiděluje IP adresy a jiné informace zařízením ve stejném síťovém segmentu, je v tuto chvíli zařízení úspěšně připojeno do sítě. Síťový provoz je poté možno zkoumat právě skrze zmíněný router.

Má situace je ovšem rozdílná oproti výše zmíněné, protože nemám fyzický přístup k takovému routeru, čímž mi je znemožněno analyzovat jeho síťový provoz. Avšak mám možnost drátového připojení skrze datovou zásuvku i bezdrátového připojení. Proto se poměrně jednoduchým řešením může zdát připojení mobilního telefonu k Wi-Fi síti a následné nastavení IP adresy výchozí brány na hodnotu IP adresy drátového rozhraní počítače, které bude připojeno do Internetu. Řešení bude na první pohled vyhovující. Detailnější rozbor ovšem upozorní na zásadní nedokonalost. Problém této konfigurace spočívá v tom, že mobilní telefon v moment, kdy se z něj odešle paket skrze drátové rozhraní počítače až do Internetu, může očekávat odpověď. Tato odpověď dorazí na router poskytující bezdrátové připojení a jelikož on má informaci o tom, že k němu je připojen mobilní telefon prostřednictvím Wi-Fi sítě, odešle mu odpověď přímo. Počítač je zcela vynechán, čímž tedy přicházím o přístup k odpovědi, která byla určena telefonu. To značně omezuje síťový monitoring, protože by byla zachycena pouze část komunikace, což není žádoucí. Proto je potřeba přijít se sofistikovanějším řešením.

## 5.2 Výsledná síť

Výsledná síť využije toho, že z počítače je Internet dosažitelný drátově a bezdrátové připojení není využito. Proto z něj vytvořím AP, který bude vysílat signál pro bezdrátové připojení. Pro jednoduchou správu také zprovozním službu DHCP, která bude distribuovat

1. rozsah IP adres 10.0.0.1–10.0.0.5, přičemž poslední z nich je přidělena mobilnímu telefonu po celou dobu všech měření,
2. masku podsítě (číslo oddělující adresu sítě a zařízení) 255.255.255.0,
3. výchozí bránu 10.0.0.1,
4. DNS (Domain Name System) server dle konfigurace sítě, v níž se nacházím.

Jen s touto konfigurací by si AP nevystačil, protože by na Internet nepřeposílal žádnou komunikaci z telefonu. Proto je potřeba ještě v systému firewall, který řídí a zabezpečuje síťový provoz na zařízení, nastavit

1. příjem komunikačního protokolu TCP (Transmission Control Protocol),
2. příjem komunikačního protokolu UDP (User Datagram Protocol),
3. příjem odpovědí komunikace, která byla iniciována mobilním telefonem,
4. příjem komunikace, která pochází přímo z mobilního telefonu,
5. přeposílání z bezdrátového síťového rozhraní na drátové,
6. odmítnutí komunikace diagnostického protokolu ICMP (Internet Control Message Protocol),
7. NAT (Network Address Translation) na drátovém rozhraní.

Zároveň je třeba si ohlídat, aby se nová nastavení navzájem nevylučovala s existujícími.

S touto konfigurací jsem dosáhl toho, že přes počítač proudí veškerá síťová komunikace, která souvisí s mobilním telefonem.

# Kapitola 6
# Měření

Tato kapitola se věnuje popisu sběru dat, problémům s ním spojených, vytipovaných IP adres a procesů mobilního telefonu, jednotlivých scénářů měření a také analýze zachycené síťové komunikace i změn ve využití systémových prostředků. Na úvod poznamenám, že veškerá měření vychází z továrního nastavení telefonu.

## 6.1 Sběr dat a jejich zpracování

Monitoring síťového provozu spočíval v pozorování bezdrátového síťového rozhraní počítače přes nástroj Wireshark. S ním byl přes Bash zároveň opakovaně spouštěn sběr dat o vytížení procesoru a operační paměti mobilního telefonu. Bylo nezbytné sbírat výpisy dat o procesoru sofistikovaněji, poněvadž k aktualizaci informací o jeho vytížení docházelo v řádu jednotek vteřin, takže nástroj nějakou dobu vracel duplikáty výsledků. Bylo tedy třeba zamezit duplikaci dat. Tato data se průběžně zpracovávala do příslušných souborů podle toho, o jaká data nebo scénář se jednalo. Ze získané síťové komunikace bylo třeba manuálně extrahovat pro následnou analýzu relevantní informace.

Pro účely vyhodnocování dat jsem v programovacím jazyce Python nad rámec zadání také vytvořil webovou aplikaci, která ovšem byla využívána pouze lokálně. Aplikace na pozadí funguje tak, že si nejprve zaznamená informace o souborech obsahující data získaná v průběhu měření a následně nad daty provede uživatelem kýžené operace. Uživatel si tak může například zvolit scénář, se kterým chce pracovat, specifikovat datum a čas začátku měření i datum a čas jeho konce nebo seskupit data po specifikovaném počtu hodin v rámci dne. Implementoval jsem také možnost porovnání dat napříč scénáři.

Jakmile aplikace skončí se zpracováním dat, dojde k jejich vykreslení do grafů. Jelikož je knihovna Plotly interaktivní, tak si uživatel může graf detailněji prohlížet – přibližovat, oddalovat, posouvat, případně po přesunutí kurzoru na vykreslený obrazec se mu zobrazí podrobnější informace, které s daným obrazcem souvisí. Snímky zachycující vzhled aplikace lze nalézt v příloze A. Veškeré vygenerované grafy, ač v lehce odlišné podobě, jsou výstupem právě této aplikace.

## 6.2 Jednoznačnost domén

Původním záměrem bylo monitorovat komunikaci pouze na základě IP adres a doménová jména zpětně dohledávat. Jelikož se v průběhu měření vyskytovalo hned několik IP adres ve vlastnictví Google, nastala jedna potíž. Při zpětném dohledávání doménových jmen bylo zjištěno, že Google z bezpečnostních důvodů využívá pro člověka obtížně čitelné domény, z nichž nelze jednoznačně

vyčíst, případně u většiny ani dohledat jejich skutečný úděl [19]. Příkladem takové domény je prg03s10-in-f4.1e100.net.

Avšak zároveň byly zaznamenávány i DNS záznamy. Komunikace tohoto protokolu sestávala z požadavku ze strany mobilního telefonu a z odpovědi ze strany DNS serveru. V odpovědi na jeden požadavek (jednu doménu) může přijít více požadavků typu A, které společně udávají seznam IP adres verze 4, na kterých se daná doména vyskytuje. Nebylo vzácným jevem ani to, že na jedné IP adrese bylo registrováno více domén. Z tohoto důvodu není v některých případech možné jednoznačně určit, na kterou doménu směřoval původní paket z telefonu a bylo třeba tento fakt brát v potaz i v následné analýze. V případě, že se přistupovalo na doménu k níž neexistoval DNS záznam v průběhu měření daného scénáře, bylo potřeba doménu určit manuálně.

Výše zmíněná situace je také nakonec důvod nevyužití nástroje *pmacct*, který neumožňuje důkladnější průzkum DNS paketů. Po celou dobu měření byla komunikace tímto nástrojem sbírána, avšak nebyla využita.

**Server Name Indication extension** Pokud je v paketu uvedeno SNIe, pak se tímto atributem specifikuje doména, se kterou se odesílatel snažil navázat komunikaci pomocí protokolu TLS (Transport Layer Security).

## 6.3 Vybrané domény

Nyní si zde dovolím rozepsat vybrané domény. Poznamenávám, že k většině domén jsem nedohledal oficiální dokumentaci, proto jsem byl nucen informace o doménách dedukovat z názvů, případně z různých diskusních fór.

**ad.doubleclick.net** Doména patří společnosti DoubleClick, která patří Google. Doména slouží k přesměrování na požadovanou stránku. Google využívá doménu k evidenci aktivity uživatelů za účelem personalizace webového obsahu [20].

**googleads.g.doubleclick.net** Účel domény bude patrně podobný jako *ad.doubleclick.net*.

**pagead2.googlesyndication.com** Na této doméně jsou umístěny skripty, které vývojářům umožňují pomocí nástroje AdSense umisťovat do svých produktů automaticky generované reklamy [21].

**adservice.google.com, googleadservices.com** Z názvu se domnívám, že se jedná o domény z hlediska účelu podobné doméně *ad.doubleclick.net*.

**userlocation.googleapis.com** Z názvu lze získat představu o údělu domény. Podle dostupných informací by měla skutečně zaznamenávat zeměpisné souřadnice zařízení [22, 23].

**mobilemaps-pa-gz.googleapis.com, mobilemaps.googleapis.com** Z názvu je evidentní, že domény zpřístupňují API pro aplikaci Mapy Google.

**streetviewpixels-pa.googleapis.com** Z názvu je evidentní, že také zpřístupňuje API pro aplikaci Mapy Google.

**alcatel.tct-supportcenter.com** Jelikož Alcatel je výrobce telefonu, tak je možné, že tato doména slouží k nějaké servisní komunikaci nebo zasílání diagnostických informací.

**tclclouds.com, tclcom.com** Na těchto doménách druhého řádu se patrně nachází servery cloud úložiště. Jejich úplné názvy vyvolávají pocit, že by mohly být geograficky odděleny nebo určeny pro jiná geografická území. Avšak v průběhu měření komunikace proudila na vícero těchto domén, jejichž názvy jsou odlišné.

**googleusercontent.com** Z názvu se domnívám, že doména slouží jako úložiště uživatelského obsahu.

**mnc003.mcc230.pub.3gppnetwork.org** Byla zaznamenána komunikace na dvou subdoménách této domény, konkrétně *epdg.epc* a *config.rcs*. Ty patří společnosti Vodafone. Jejich výskyt velice pravděpodobně souvisí s přítomností Vodafone SIM karty v telefonu [24, 25].

## 6.4 Vybrané procesy

Dovolím si zmínit několik procesů. Poznamenávám, že i v tomto případě jsem byl nucen u několika procesů čerpat informace z názvů nebo diskusních fór, leč situace byla mnohem přívětivější, než u domén.

**android.hardware.audio** Tento proces se pravděpodobně věnuje práci s audio záznamy na hardware úrovni telefonu.

**android.hardware.gnss** Tento proces údajně poskytuje přístup k zeměpisným souřadnicím zařízení [26].

**android.hardware.sensors** Senzory na platformě Android jsou virtuální zařízení, která poskytují data z fyzických senzorů mobilního telefonu. Proces tedy bude nejspíše souviset s aktivitou směřovanou těmto virtuálním zařízením [27].

**android.hardware.wifi** Tento proces zprostředkovává přístup k Wi-Fi sítím [28].

**com.google.android.apps.assistant** Jedná se o aplikaci Google Assistant Go [29].

**com.google.android.apps.maps** Tento proces náleží aplikaci Mapy Google.

**com.google.android.apps.navlite** Tento proces náleží navigační aplikaci Navigation for Google Maps Go [30].

**com.google.android.tts** Tento proces náleží aplikaci Google Text-to-Speech. Využívá ji například Google překladač pro převod mluveného slova na text i opačně [31].

**system** V tomto případě se jedná o proces, který byl zaznamenán hlavně nástrojem monitorujícím spotřebu operační paměti. Spotřeba procesoru dosahovala zanedbatelných hodnot, navíc byla zjištěna zřídkakdy. Domnívám se, že se jedná o jeden z klíčových procesů operačního systému.

**system_server** Tento proces charakterizuji obdobně jako proces *system*, avšak s tím rozdílem, že tento byl zaznamenán hlavně nástrojem monitorujícím spotřebu procesoru.

**wificond** Proces komunikuje s Wi-Fi ovladači [32].

**xtra-daemon** Tento proces patrně souvisí s výrobcem procesoru, kterým je společnost Qualcomm. Údajně umožňuje rychlejší zjištění zeměpisné polohy zařízení [33].

Pro všechny procesy, které při vyhodnocení konkrétního scénáře nejsou explicitně zmíněny, platí, že vykazují podobné vlastnosti oproti předchozím scénářům nebo zaznamenaly nevýznamnou až nulovou spotřebu, nebo se dokonce v daném scénáři vůbec nevyskytovaly.

Analogické tvrzení platí i pro data spotřeby na úrovni operační paměti (Random Access Memory, RAM) a procesoru (Central Processing Unit, CPU).

## 6.5 Scénář 0

Pro získání představy o chování mobilního telefonu v „běžném“ stavu bylo provedeno počáteční měření. Charakteristiky tohoto scénáře vystihuje Tabulka 6.1. Zjednodušeně lze říci, že se nijak nezasahovalo do výchozího nastavení telefonu ani nebyly vědomě ukončovány, nebo zahajovány jakékoli procesy.

**Tabulka 6.1** Podmínky scénáře 0

| | |
|---|---|
| Určování polohy | Povoleno |
| Asistent Google Go | Povolen |
| SIM karta v telefonu | Ano |
| Aplikace na pozadí | Nezkoumány |
| Přibližná doba měření | 84 hodin |

### 6.5.1 Síťová komunikace

Z tabulky 6.2 lze vyčíst kolik bajtů bylo zachyceno při komunikaci s výše popsanými doménami i objem veškeré komunikace telefonu.

**Tabulka 6.2** Množství bajtů v komunikaci s doménami scénáře 0

| Doména | Odesláno | Přijato | SNIe |
|---|---|---|---|
| 3gppnetwork | 129 KB | 33,3 KB | 6,53 KB |
| ad.doubleclick | 158 KB | 46,9 KB | 7,75 KB |
| adservices | 234 KB | 62,5 KB | 3,84 KB |
| googleusercontent | 2,03 MB | 159 KB | 1,1 KB |
| mobilemaps | 302 KB | 191 KB | 9,5 KB |
| tclclouds, tclcom | 345 MB | 3,37 MB | 4,39 KB |
| tct-supportcenter | 89,1 KB | 28,6 KB | 7,69 KB |
| userlocation | 5,62 MB | 3,72 MB | 1,65 KB |
| Celkem | 472 MB | 10,8 MB | 530 KB |

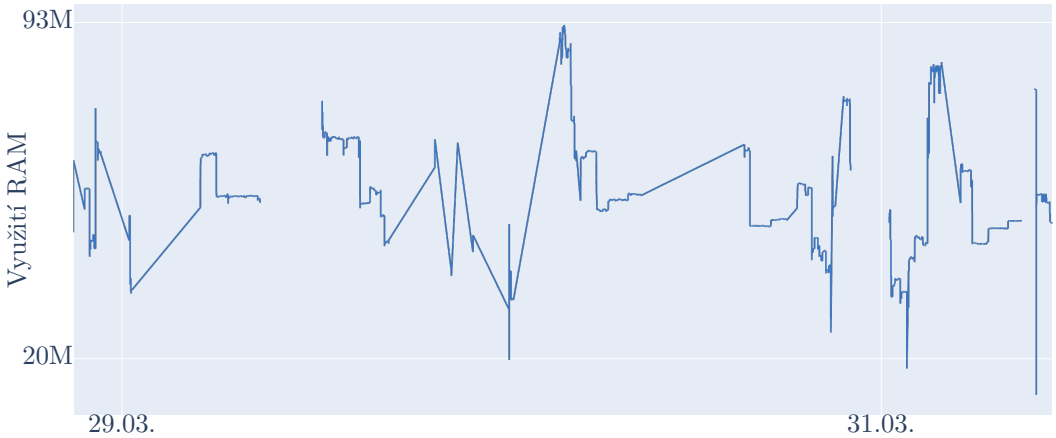
Nejprve vysvětlení záznamů v tabulce, doména mnc003.mcc230.pub.3gppnetwork.org je skryta pod záznamem *3gppnetwork*. Záznam *ad.doubleclick* obsahuje referenci na doménu ad.doubleclick.net. Záznam *adservices* odkazuje na domény adservice.google.com, googleads.g.doubleclick.net (ta je zahrnuta pod tímto záznamem, protože sdílí IP adresu se zbylými doménami *adservices*), googleadservices.com a pagead2.googlesyndication.com, přičemž ne každý scénář zaznamenal komunikaci se všemi doménami. Záznam *googleusercontent* odkazuje na doménu googleusercontent.com. Záznam *mobilemaps* odkazuje na domény mobilemaps-pa-gz.googleapis.com, mobilemaps.googleapis.com, streetviewpixels-pa.googleapis.com a gz0.googleusercontent.com, přičemž platí, že poslední 2 zmíněné domény se vyskytují zřídka. Poslední zmíněná doména není zahrnutá pod *googleusercontent*, protože analýzou DNS záznamů jsem došel k zjištění, že tato doména sdílí IP adresy s ostatními doménami záznamu *mobilemaps*. Záznam *tclclouds,*

*tclcom* odkazuje na domény tclclouds.com a tclcom.com. Záznam *tct-supportcenter* odkazuje na doménu alcatel.tct-supportcenter.com a konečně záznam *userlocation* odkazuje na doménu userlocation.googleapis.com. U této domény si ještě dovolím zmínit, že zde v každém scénáři, kde byl zjištěn výskyt domény, dochází k nejednoznačnosti, což je popsáno v 6.2.

Pokud jde o hodnoty přenesených dat, tak je na první pohled zarážející objem odeslaných dat z *tclclouds, tclcom*. Konstatuji, že v časovém rozmezí, ve kterém byla zaregistrována drtivá většina této komunikace proběhla aktualizace operačního systému. Domnívám se, že tyto události spolu mohou souviset. Připomínám, že u *userlocation* není možné určit přesný objem komunikace související s doménou userlocation.googleapis.com, avšak podle celkové velikosti paketů se specifikovaným atributem SNIe je vidět, že nějaká komunikace na tuto doménu skutečně směřovala. Objem přenesených dat ostatních domén se mi jeví očekávaný.

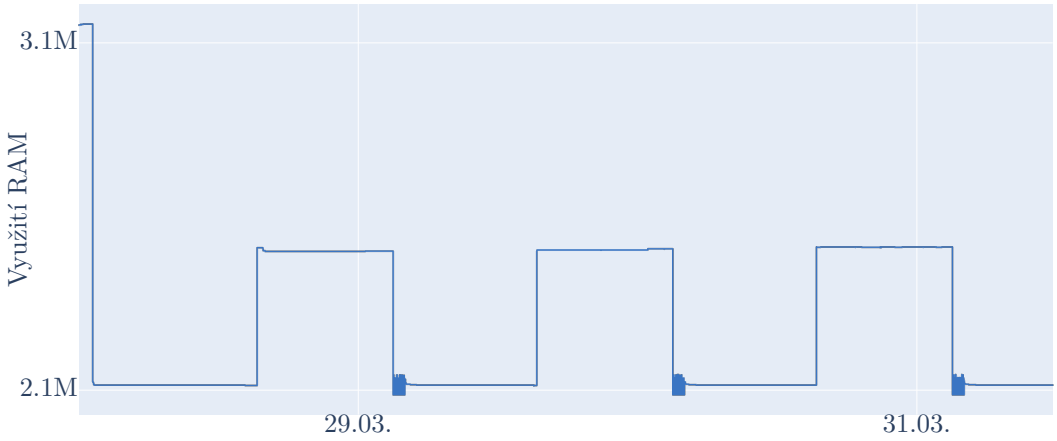
### 6.5.2 Využití systémových prostředků

Obrázek 6.1 ukazuje jistou nestabilitu ve vytížení RAM zapříčiněnou mapovou aplikací. Tato nestabilita pravděpodobně znamená, že Mapy Google střídavě vykonávaly nějakou aktivitu, ač celou dobu byly spuštěny nanejvýše na pozadí telefonu. Jedná se o jev, který bude nadále zkoumán.



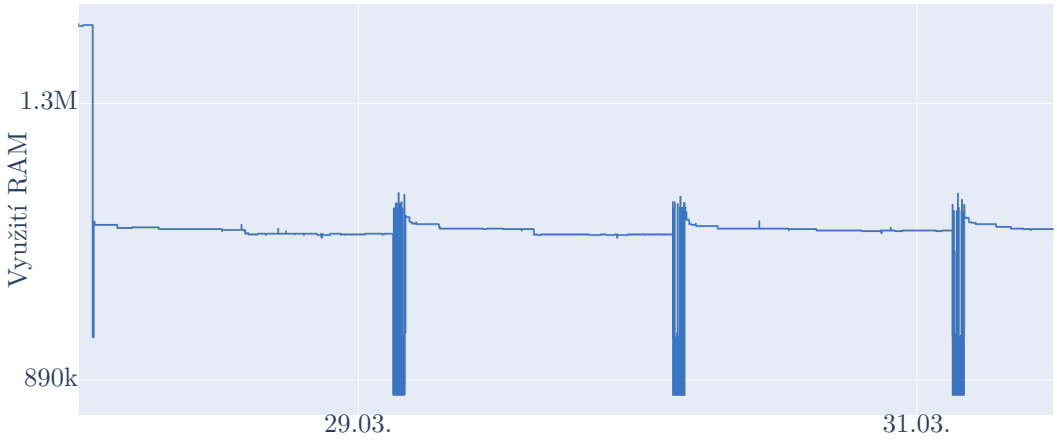

**Obrázek 6.1** Scénář 0: využití RAM procesem com.google.android.apps.maps

Proces *android.hardware.gnss* periodicky zvyšoval svou spotřebu zhruba o 0,3 MB kolem 15. hodiny, přičemž pokles následoval kolem 3. hodiny ranní.



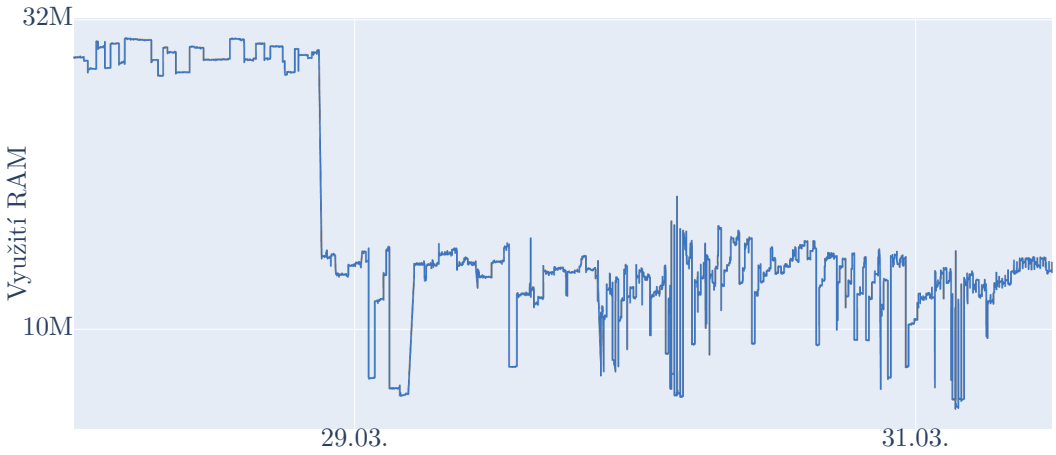

**Obrázek 6.2** Scénář 0: využití RAM procesem android.hardware.gnss

Nebyla zjištěna významná spotřeba RAM procesem *android.hardware.wifi*, nicméně jak ukazuje Obrázek 6.3, byla zjištěna periodicita mezi 3. až 4. hodinou ranní.



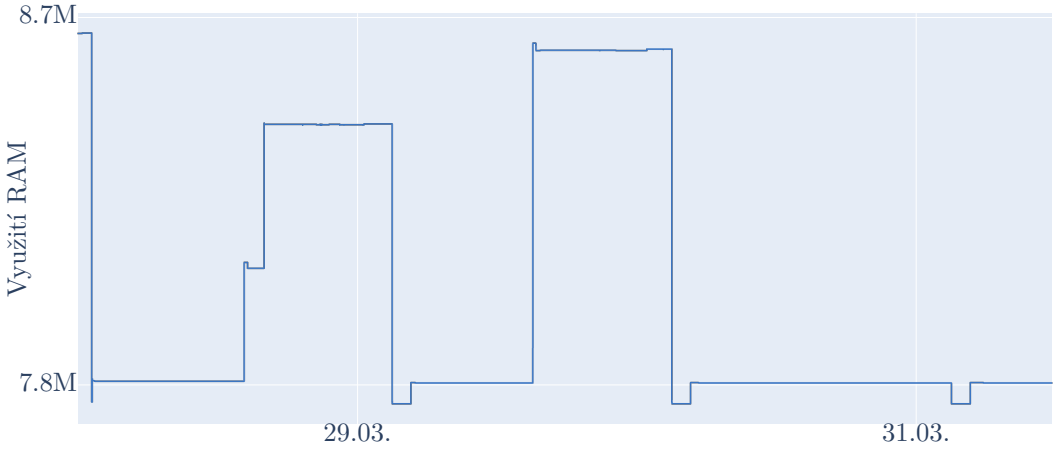

**Obrázek 6.3** Scénář 0: využití RAM procesem android.hardware.wifi

Obrázek 6.4 ukazuje, že vytížení RAM procesem *com.google.android.tts* mělo v úvodních 24 hodinách měření dvojnásobně vyšší aktivitu, než ve zbytku tohoto scénáře. Až na prvních 24 hodin měření bylo pak také každý den kolem 3. až 4. hodiny ranní zaznamenáno snížení spotřeby směrem k minimu, zatímco výraznější zvýšení se dále nevyskytlo.

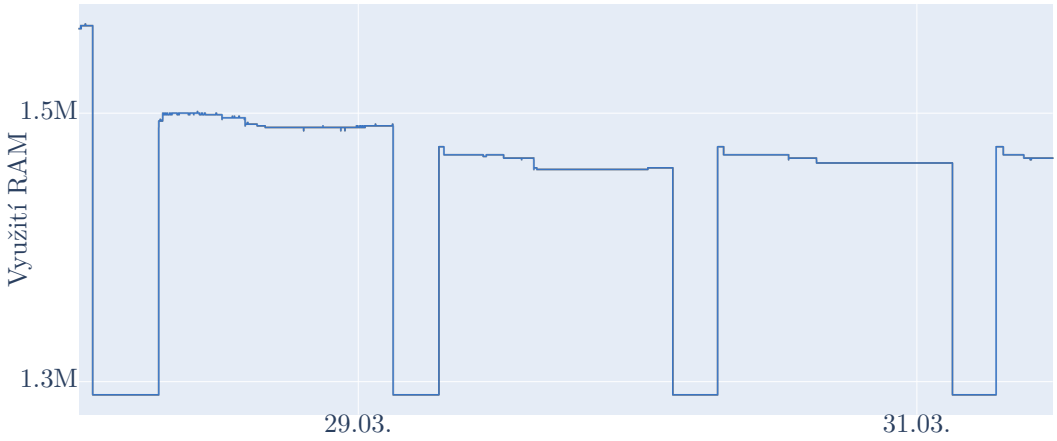



**Obrázek 6.4** Scénář 0: využití RAM procesem com.google.android.tts

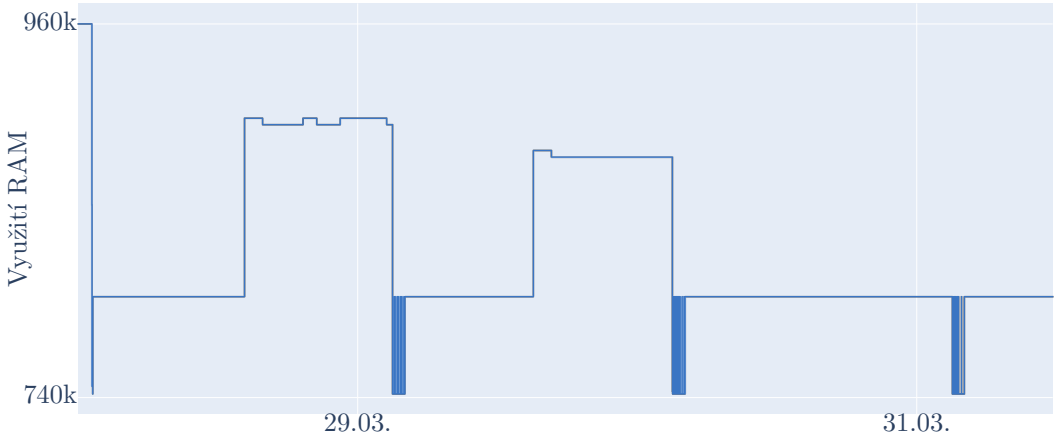
Dále byly zaznamenány aktivity procesů *android.hardware.audio*, *android.hardware.sensors* a *wificond*, přičemž každý z nich vykazoval jisté známky periodicity.




**Obrázek 6.5** Scénář 0: využití RAM procesem android.hardware.audio




**Obrázek 6.6** Scénář 0: využití RAM procesem android.hardware.sensors




**Obrázek 6.7** Scénář 0: využití RAM procesem wificond

Z vytížení jiných procesů nebylo možné cokoli vyčíst, vzhledem k faktu, že se jednalo o úvodní měření.

## 6.6 Scénář 1

Charakteristika tohoto scénáře se oproti 6.5 liší v zákazu určování polohy.

**Tabulka 6.3** Podmínky scénáře 1

| | |
|---|---|
| Určování polohy | Zakázáno |
| Asistent Google Go | Povolen |
| SIM karta v telefonu | Ano |
| Aplikace na pozadí | Nezkoumány |
| Přibližná doba měření | 120 hodin |

### 6.6.1 Síťová komunikace

Množství bajtů v komunikaci s vybranými doménami zachycuje Tabulka 6.4.

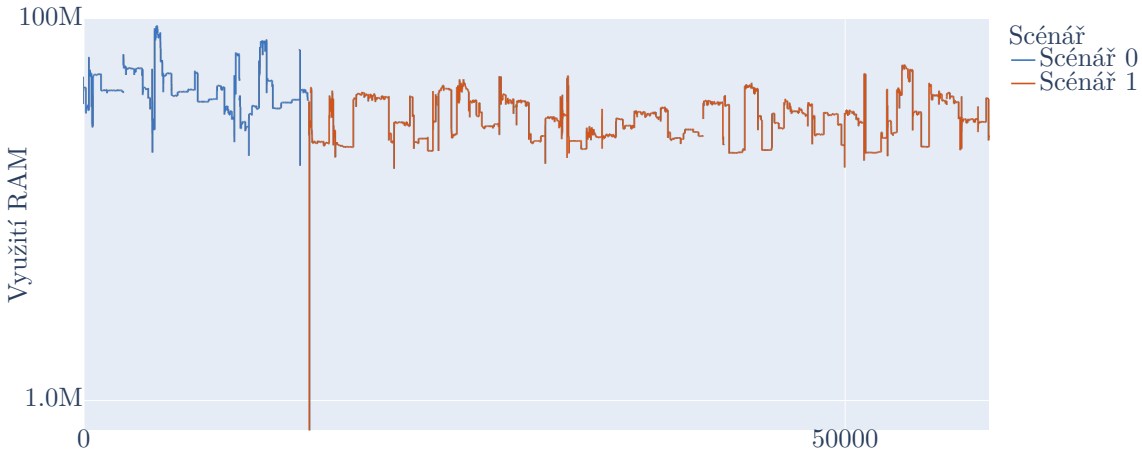
**Tabulka 6.4** Množství bajtů v komunikaci s doménami scénáře 1

| Doména | Odesláno | Přijato | SNIe |
|---|---|---|---|
| 3gppnetwork | 149 KB | 38,3 KB | 7,5 KB |
| ad.doubleclick | 180 KB | 47,3 KB | 12,4 KB |
| adservices | 560 KB | 148 KB | 26,3 KB |
| googleusercontent | 185 KB | 34,1 KB | 1,65 KB |
| mobilemaps | 514 KB | 255 KB | 15,5 KB |
| tclclouds, tclcom | 26,1 KB | 7,02 KB | 2,74 KB |
| tct-supportcenter | 121 KB | 28,3 KB | 10,4 KB |
| userlocation | 12,2 MB | 11,2 MB | 2,2 KB |
| Celkem | 185 MB | 11,9 MB | 555 KB |

Doména pagead2.googlesyndication.com se tentokráte v komunikaci vůbec nevyskytuje. Doba měření je oproti předcházejícímu scénáři přibližně o polovinu delší. Tomuto poměru zhruba odpovídá i komunikace domény alcatel.tct-supportcenter.com, u domény 3gppnetwork.org byl zaznamenán o něco nižší nárůst. Jeví se jako pravděpodobné, že googleusercontent.com reaguje na změnu oprávnění určování polohy, kvůli řádově nižšímu objemu komunikace. Záznam *ad.doubleclick* zaznamenal nižší nárůst, než bylo očekáváno, naopak *adservices* mnohem vyšší. Celkový objem telefonem přijatých dat se výrazně snížil, zejména výrazným poklesem komunikace domén tclcloud.com a tclcom.com, kdy byla v tomto scénáři zaznamenána pouze 1 jejich subdoména. Doména userlocation.googleapis.com je ovlivněna nejednoznačností, nicméně stále zde probíhalo spojení podle atributu SNIe, což se dá označit za neočekávané chování, vzhledem k vypnutému určování polohy. Pokud jde o *mobilemaps*, tak byl zaznamenán nárůst odchozí komunikace, ale pokles přijaté. Cílem vypnutí oprávnění k určení polohy ale byl mnohem výraznější pokles všech 3 druhů komunikace, nebo jeho úplné vymizení, což nenastalo.

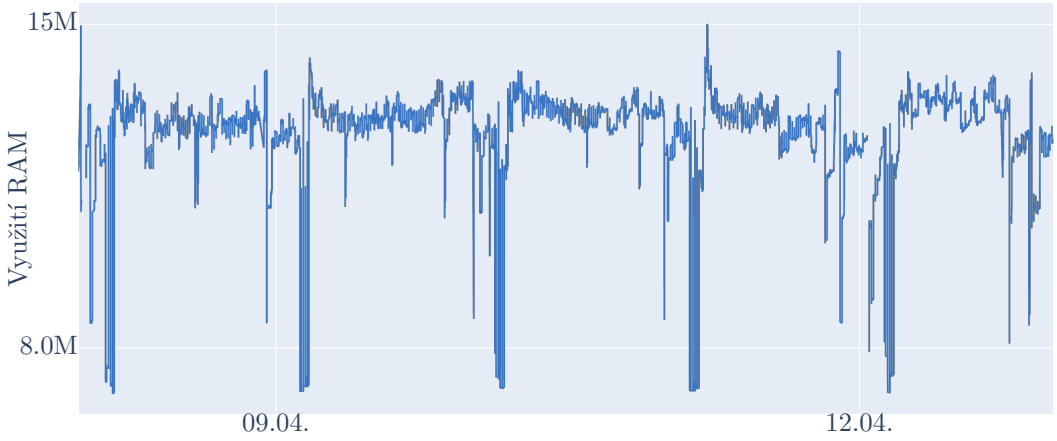
### 6.6.2 Využití systémových prostředků

Srovnání vytížení RAM procesem *com.google.android.apps.maps* se záznamy předchozího scénáře nabízí Obrázek 6.8. Průměrné využití operační paměti se sice oproti předchozímu měření snížilo o 14 MB, avšak množství záznamů oproti původnímu scénáři narostlo přibližně 4x. Byl očekáván nižší nárůst počtu záznamů, vzhledem k délce měření.




**Obrázek 6.8** Scénáře 0, 1: využití RAM procesem com.google.android.apps.maps

U procesu *com.google.android.tts* bylo v očekávaném poměru zaznamenáno zvýšení záznamů spotřeby RAM, o 3,6 MB bylo sníženo i průměrně vytížení. To je zapříčiněno tím, že proces v tomto měření nezaznamenal výraznější navýšení. Během měření nadále pokračoval periodický útlum mezi 3. až 4. hodinou ranní.

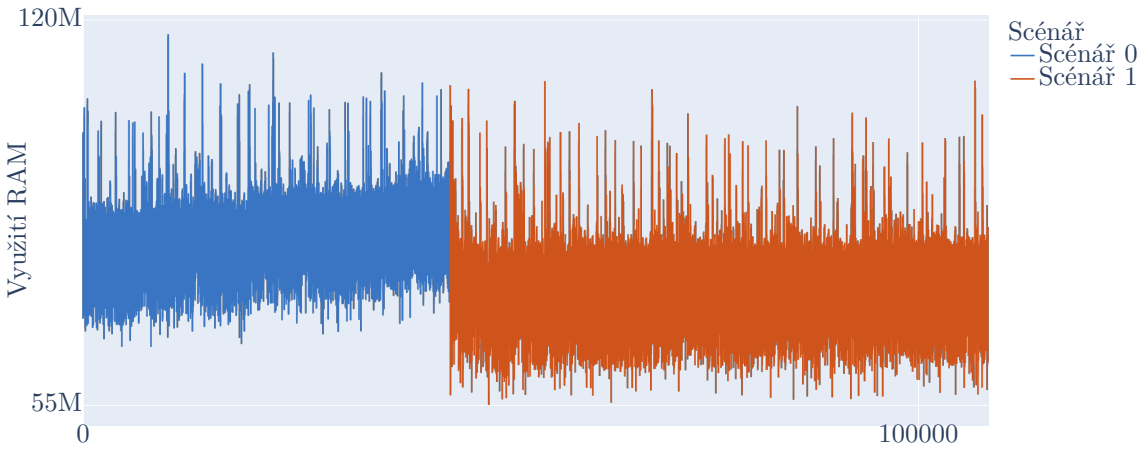



**Obrázek 6.9** Scénář 1: využití RAM procesem com.google.android.tts

Zatímco v předchozím scénáři proces *com.google.android.apps.assistant* takřka neexistoval, v nynějším měření se proces začal objevovat v součtu alespoň na hodinu každých 24 hodin.

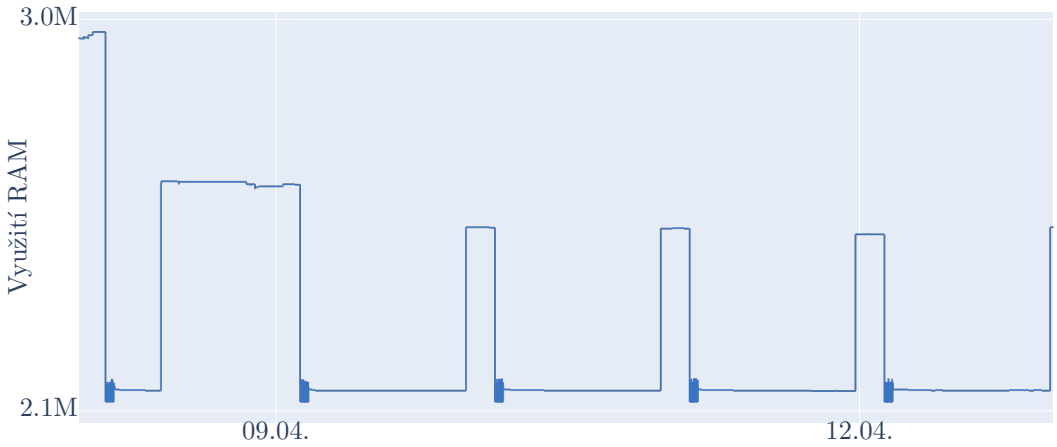

**Obrázek 6.10** Scénář 1: využití RAM procesem com.google.android.apps.assistant

Srovnání procesu *system* ukazuje, že zareagoval snížením průměrné spotřeby operační paměti o 10 %.




**Obrázek 6.11** Scénáře 0, 1: využití RAM procesem system

U procesu *android.hardware.gnss* byla zaznamenána změna periodického chování, začátek zvyšování spotřeby byl posunut na 23:26h.




**Obrázek 6.12** Scénář 1: využití RAM procesem android.hardware.gnss

## 6.7 Scénář 2

Scénář navazuje na předchozí scénář 6.6, když v něm byly zakázány aplikace Asistent Google Go a Hlasové služby od Googlu.

**Tabulka 6.5** Podmínky scénáře 2

| | |
|---|---|
| Určování polohy | Zakázáno |
| Asistent Google Go | Zakázán |
| Hlasové služby od Googlu | Zakázány |
| SIM karta v telefonu | Ano |
| Aplikace na pozadí | Nezkoumány |
| Přibližná doba měření | 40 hodin |

### 6.7.1 Síťová komunikace

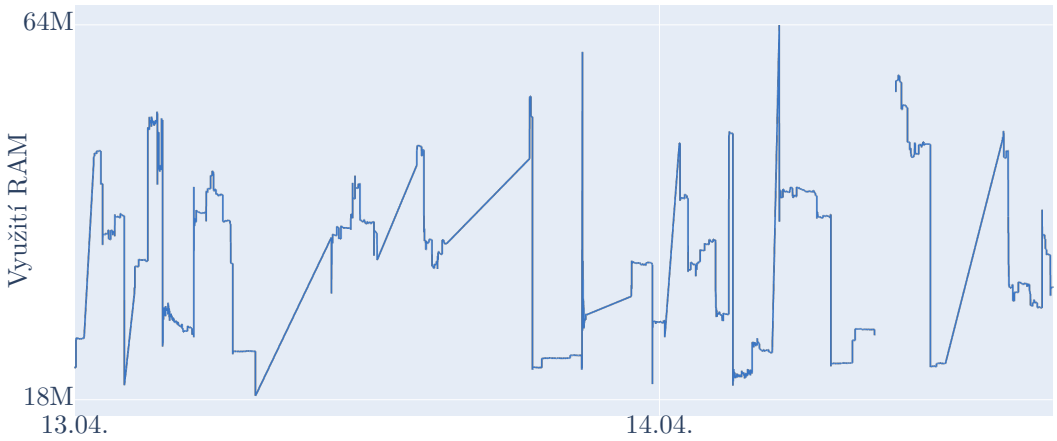
**Tabulka 6.6** Množství bajtů v komunikaci s doménami scénáře 2

| Doména | Odesláno | Přijato | SNIe |
|---|---|---|---|
| 3gppnetwork | 29,1 KB | 7,42 KB | 1,45 KB |
| ad.doubleclick | 27,6 KB | 5,9 KB | 4,26 KB |
| adservices | 110 KB | 32,2 KB | 10,7 KB |
| googleusercontent | 110 KB | 13 KB | 549 B |
| mobilemaps | 230 KB | 112 KB | 7,14 KB |
| tclclouds, tclcom | 12,9 KB | 3,43 KB | 1,1 KB |
| tct-supportcenter | 44,6 KB | 10,4 KB | 3,84 KB |
| userlocation | 2,37 MB | 2,89 MB | 1,1 KB |
| Celkem | 42 MB | 4,51 MB | 205 KB |

Objem, zejména odchozí, komunikace *ad.doubleclick*, *adservices* a *googleusercontent* klesl nad očekávání. Očekávaný výsledek tohoto měření obsahoval snížení komunikace *tct-supportcenter* i *3gppnetwork* na třetinu oproti předchozímu scénáři, což nastalo. Dále se snížila, byť trochu méně, i komunikace *tclclouds* a *tclcom*. Naměřené hodnoty z původního scénáře v řádu stovek MB se tedy skutečně začínají jevit jako anomálie. Výrazněji se snížila komunikace skupin domén, které sídlí na stejných IP adresách jako *userlocation*. I přes ponechání oprávnění pro určení zeměpisné polohy ve vypnutém stavu se nadále vyskytuje komunikace *mobilemaps* (stejně jako SNIe při *userlocation*), byť se také snížila, ač ne tak proporčně.

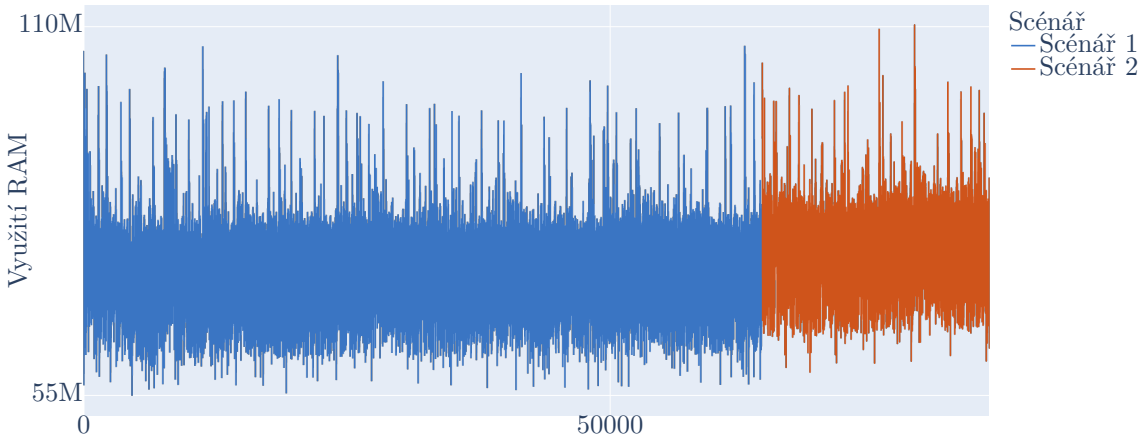
### 6.7.2 Využití systémových prostředků

Průměrná spotřeba RAM procesem *com.google.android.apps.maps* zůstala oproti předchozímu měření téměř beze změny, naopak počet záznamů klesl dle očekávání.




**Obrázek 6.13** Scénář 2: využití RAM procesem com.google.android.apps.maps

Průměrná spotřeba RAM procesem *system* mírně vzrostla, nicméně pouze o 3 MB, což nepovažuji za nijak zásadní.




**Obrázek 6.14** Scénáře 1, 2: využití RAM procesem system

## 6.8 Scénář 3

Jediné změny oproti předchozímu nastavení 6.7 spočívají v měření komunikace při spuštěné aplikaci Mapy Google na popředí telefonu a samozřejmě povolením zjišťování zeměpisné polohy.

**Tabulka 6.7** Podmínky scénáře 3

| | |
|---|---|
| Určování polohy | Povoleno |
| Asistent Google Go | Zakázán |
| Hlasové služby od Googlu | Zakázány |
| SIM karta v telefonu | Ano |
| Aplikace na pozadí | Nezkoumány |
| Mapy Google na popředí | Ano |
| Přibližná doba měření | 48 hodin |

### 6.8.1 Síťová komunikace

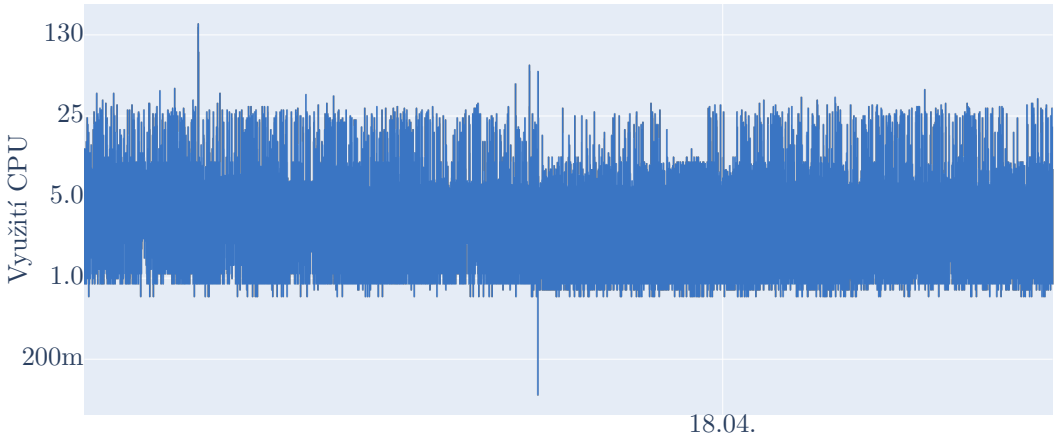
**Tabulka 6.8** Množství bajtů v komunikaci s doménami scénáře 3

| Doména | Odesláno | Přijato | SNIe |
|---|---|---|---|
| 3gppnetwork | 4,79 KB | 1,24 KB | 240 BB |
| ad.doubleclick | 102 KB | 32,4 KB | 4,69 KB |
| adservices | 202 KB | 60,9 KB | 12,9 KB |
| googleusercontent | 147 KB | 48,3 KB | 549 B |
| mobilemaps, streetview | 2,52 MB | 2 MB | 2,37 KB |
| tclclouds, tclcom | 13,1 KB | 3,51 KB | 1,1 KB |
| tct-supportcenter | 51,1 KB | 12,2 KB | 4,39 KB |
| userlocation | 3,23 MB | 3,31 MB | 1,1 KB |
| Celkem | 15,3 MB | 7,07 MB | 168 KB |

I přes prodloužení doby měření a spuštěnou aplikaci Mapy Google na popředí byl zaznamenán výrazný pokles provozu směrem do telefonu. Dle očekávání se zvýšil objem dat odeslaných telefonem. Doména userlocation.googleapis.com zůstala podle SNIe nadále aktivní, řádově vzrostl objem dat komunikace související s aplikací Mapy Google. Ač v tomto případě se k jedné IP adrese hlásily navíc domény streetview.googleapis.com a gz0.googleusercontent.com. Posledně zmíněná doména, jak bylo zmíněno v části 6.3, slouží jako úložiště uživatelského obsahu. Tudíž se domnívám, že její výskyt, pakliže skutečně souvisí s mapovou aplikací, může být odůvodněn kupříkladu uživatelskými recenzemi podniků v blízkém okolí aplikace v průběhu měření. Vypadá to, že subdomény googleusercontent.com (vyjma zmíněné gz0) nijak nereagují na aktivitu mapové aplikace. U domén spadajících pod skupiny *adservices* a *ad.doubleclick* bylo spatřeno výraznější navýšení komunikace. Zbylé domény buď snížily objem komunikace, nebo si jej v podobných hodnotách zachovaly.

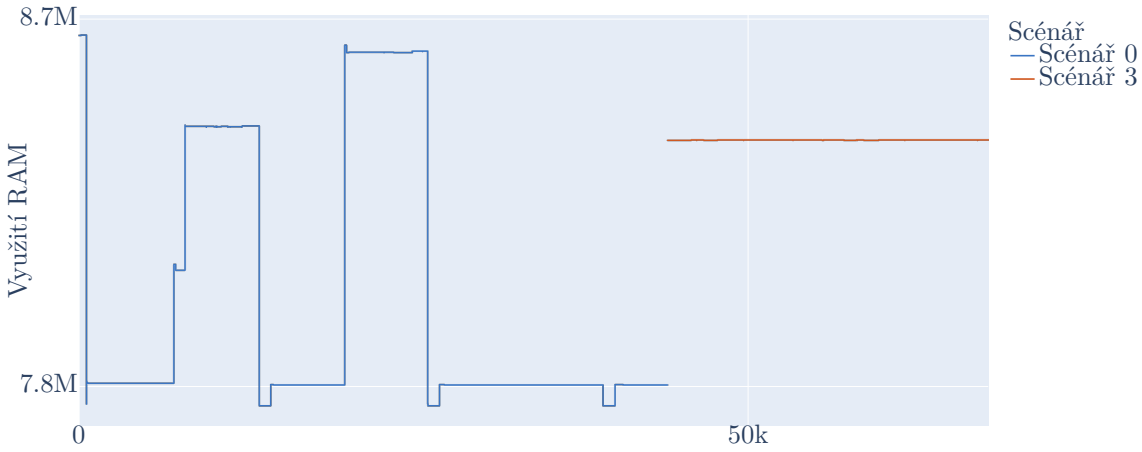
### 6.8.2 Využití systémových prostředků

Tentokráte nebyl vůbec zjištěn výskyt procesu *com.google.android.apps.maps* při měření spotřeby operační paměti, avšak spotřeba procesoru ukazuje přes 30 tisíc záznamů s průměrem pod 4 %.



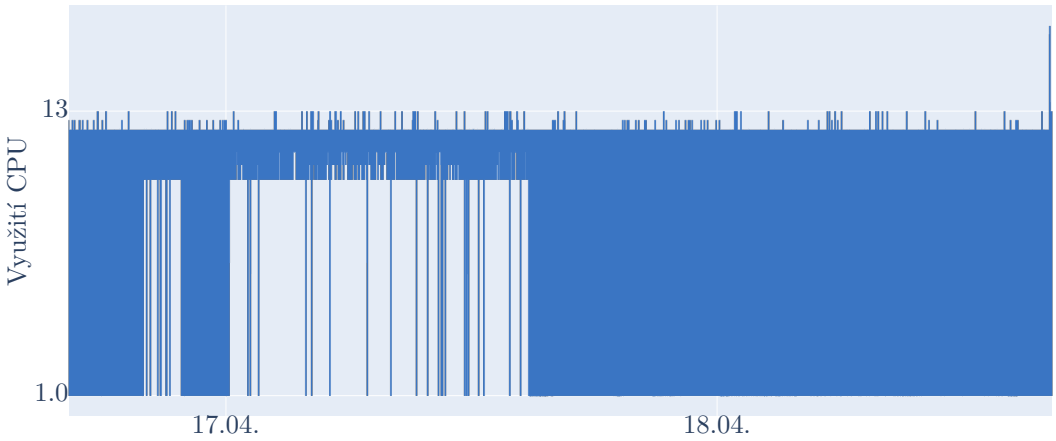

**Obrázek 6.15** Scénář 3: využití CPU procesem com.google.android.apps.maps

Spotřeba RAM procesem *android.hardware.audio* zůstala po dobu měření téměř neměnná a po většinu času oproti 6.5 navíc výrazně vyšší.

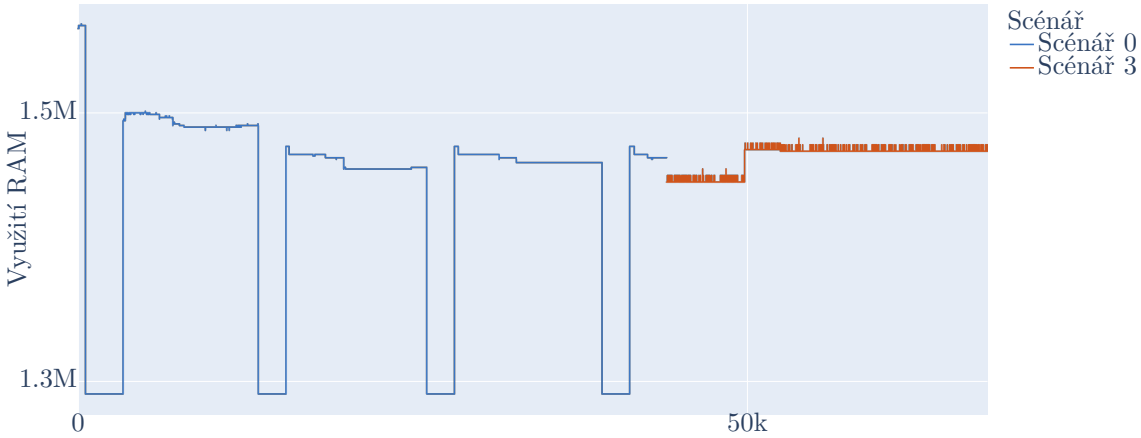



**Obrázek 6.16** Scénář 0, 3: využití RAM procesem android.hardware.audio

Spotřeby *android.hardware.sensors* také doznaly významných změn. Byla naměřena významná spotřeba CPU a spotřeba RAM oproti běžnému stavu 6.6 zároveň oscilovala na mnohem menším intervalu.



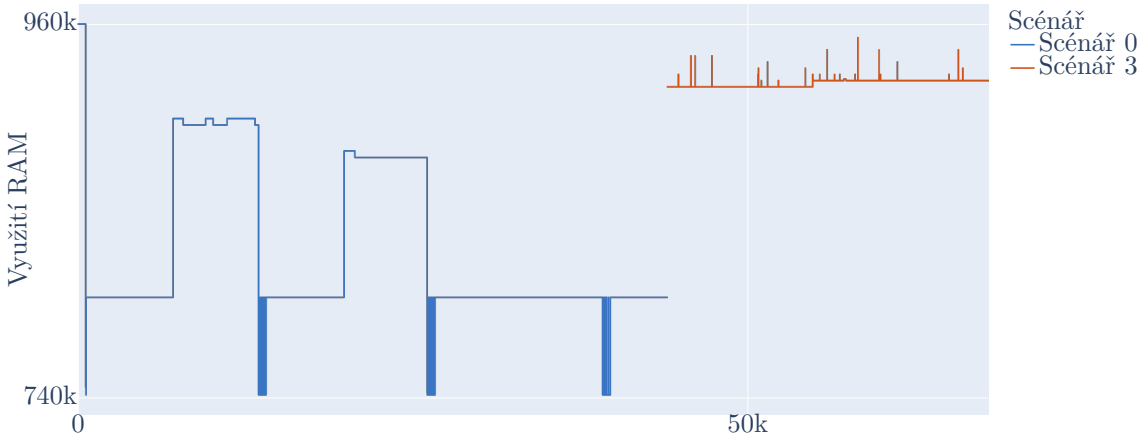

**Obrázek 6.17** Scénář 3: využití CPU procesem android.hardware.sensors




**Obrázek 6.18** Scénáře 0, 3: využití RAM procesem android.hardware.sensors

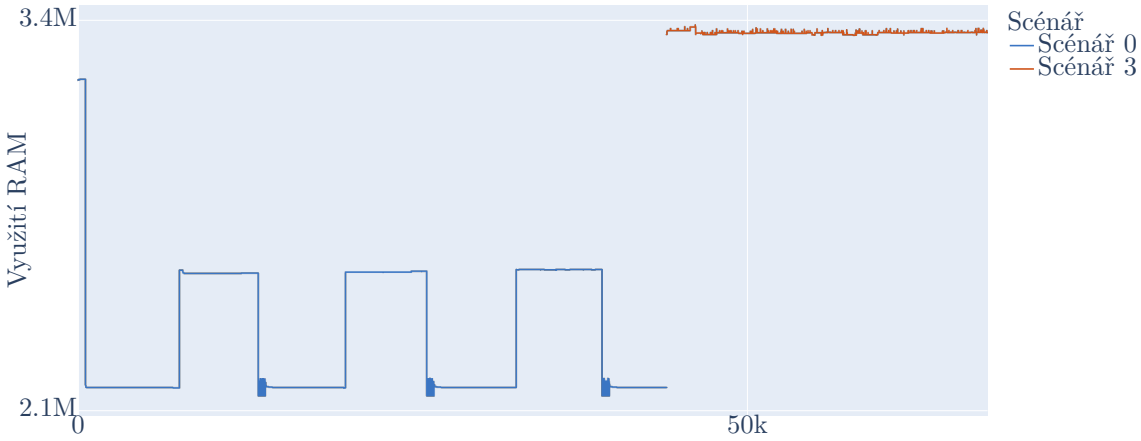
Obdobně procesu *android.hardware.sensors* se změnilo i vytížení procesoru a operační paměti u *wificond*.


**Obrázek 6.19** Scénář 3: využití CPU procesem wificond



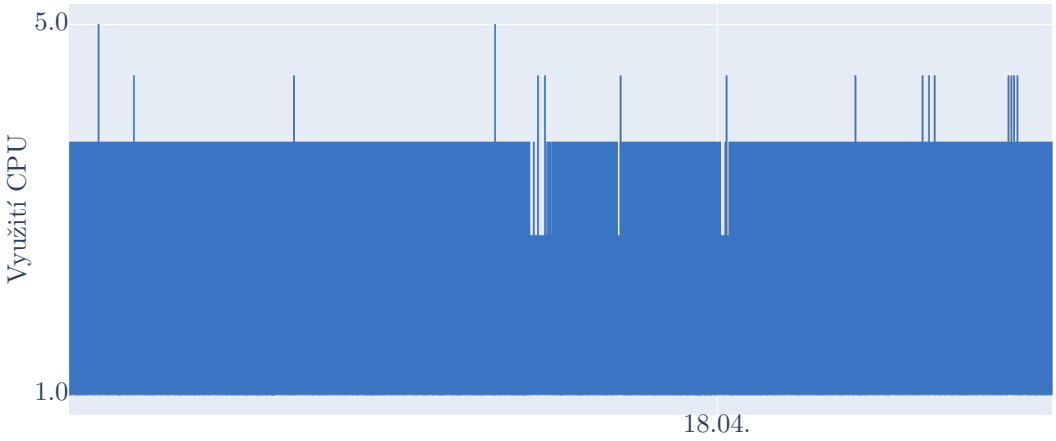

**Obrázek 6.20** Scénáře 0, 3: využití RAM procesem wificond

Oproti 6.2 se také o 50 % zvýšila spotřeba RAM procesem *android.hardware.gnss*.



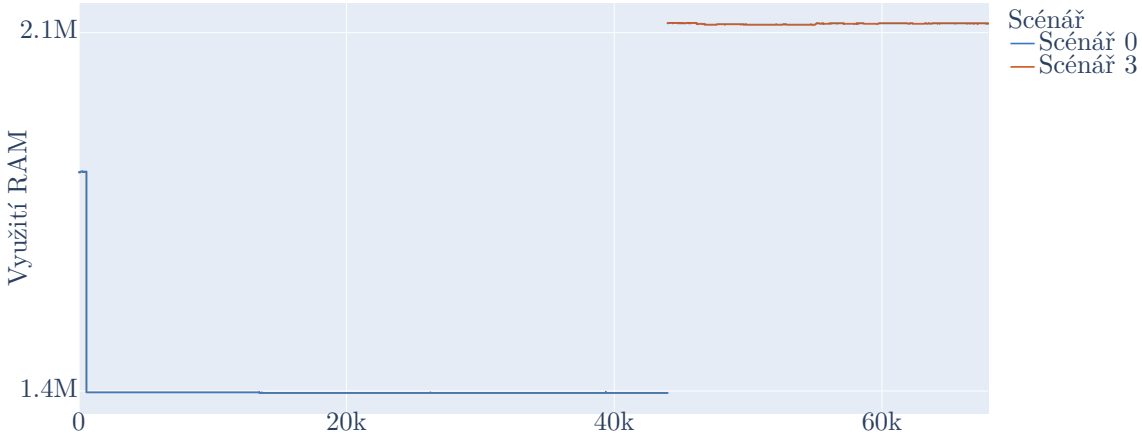

**Obrázek 6.21** Scénáře 0, 3: využití RAM procesem android.hardware.gnss

Stejně tak u něj byla zaznamenána významná aktivita CPU po celou dobu měření scénáře.



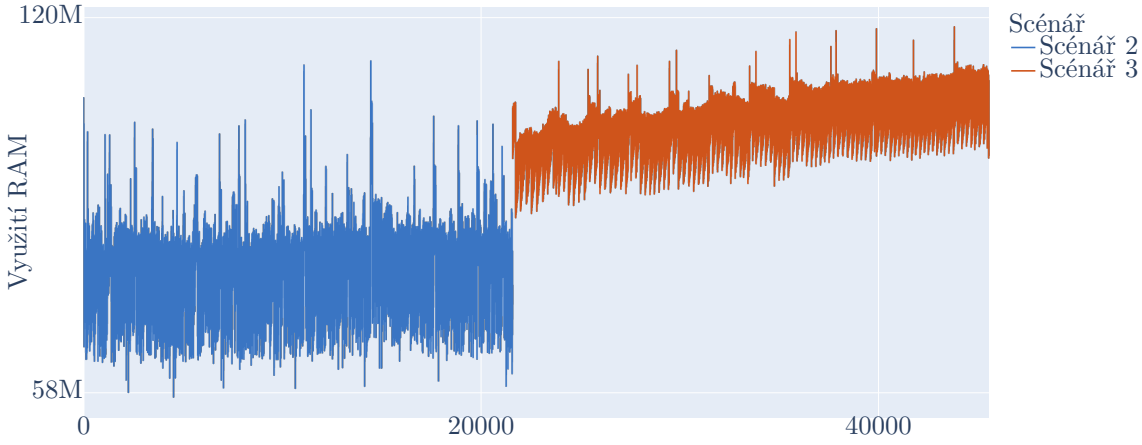

**Obrázek 6.22** Scénář 3: využití CPU procesem android.hardware.gnss

Proces *xtra-daemon* si zachovával poměrně stabilní zvýšenou spotřebu operační paměti v průběhu měření. Tento děj spojuji s aktivní aplikací Mapy Google.




**Obrázek 6.23** Scénář 3: využití RAM procesem xtra-daemon

V souladu s očekáváním významně, o 25 MB v průměru, stoupla spotřeba operační paměti v rámci procesu *system*.




**Obrázek 6.24** Scénáře 2, 3: využití RAM procesem system

## 6.9 Scénář 4

Toto měření bylo oproti 6.8 pozměněno ukončením aplikací běžících na pozadí. Ukončením se myslí způsob, kdy se zmáčknutím některého z domovských tlačítek zobrazí seznam procesů, které běží na pozadí a posunutím okna s aplikací nahoru se aplikace ukončí. Respektive ukončení bych očekával.

**Tabulka 6.9** Podmínky scénáře 4

| | |
|---|---|
| Určování polohy | Zakázáno |
| Asistent Google Go | Zakázán |
| Hlasové služby od Googlu | Zakázány |
| SIM karta v telefonu | Ano |
| Aplikace na pozadí | Žádné |
| Přibližná doba měření | 28 hodin |

### 6.9.1 Síťová komunikace

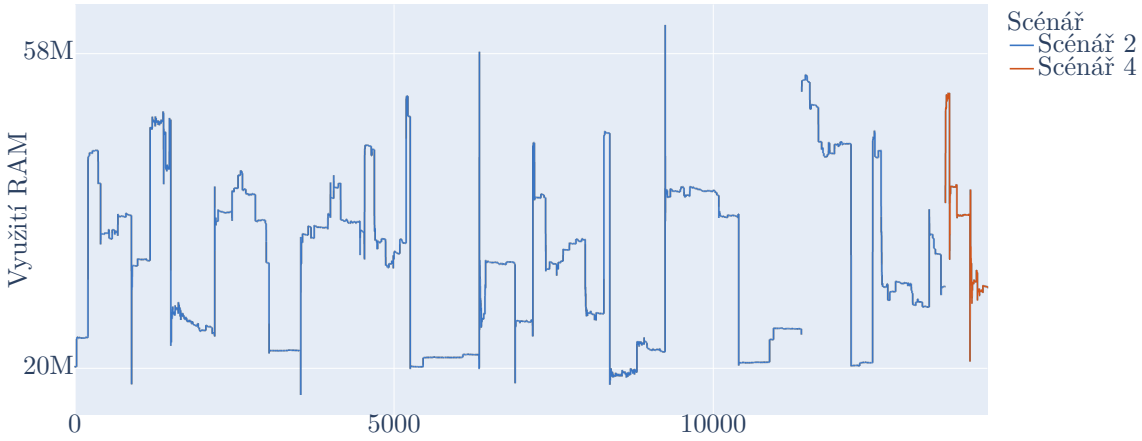
**Tabulka 6.10** Množství bajtů v komunikaci s doménami scénáře 4

| Doména | Odesláno | Přijato | SNIe |
|---|---|---|---|
| 3gppnetwork | 4,79 KB | 1,24 KB | 242 B |
| ad.doubleclick | 30,7 KB | 10,3 KB | 3,28 KB |
| adservices | 114 KB | 29,9 KB | 5,49 KB |
| googleusercontent | 6,42 KB | 3,07 KB | 0 B |
| mobilemaps | 38,2 KB | 28,6 KB | 1,1 KB |
| tclclouds, tclcom | 13,1 KB | 3,51 KB | 549 B |
| tct-supportcenter | 25,5 KB | 5,63 KB | 2,2 KB |
| userlocation | 652 KB | 532 KB | 549 B |
| Celkem | 91,9 MB | 2,76 MB | 133 KB |

U záznamů *3gppnetwork*, *tclclouds, tclcom* a *tct-supportcenter* lze stále spatřovat jisté podobnosti. Významný pokles oproti scénáři 6.7, který je srovnatelný s tímto, nastal u *mobilemaps*, nicméně stále se alespoň nějaká komunikace zachovává. Domény zahrnuty pod *ad.doubleclick* a *adservices* zřejmě nereagují ani na ukončení aplikací na pozadí ve srovnání s předchozím scénářem. Doména googleusercontent.com zaznamenala významný pokles veškeré komunikace.

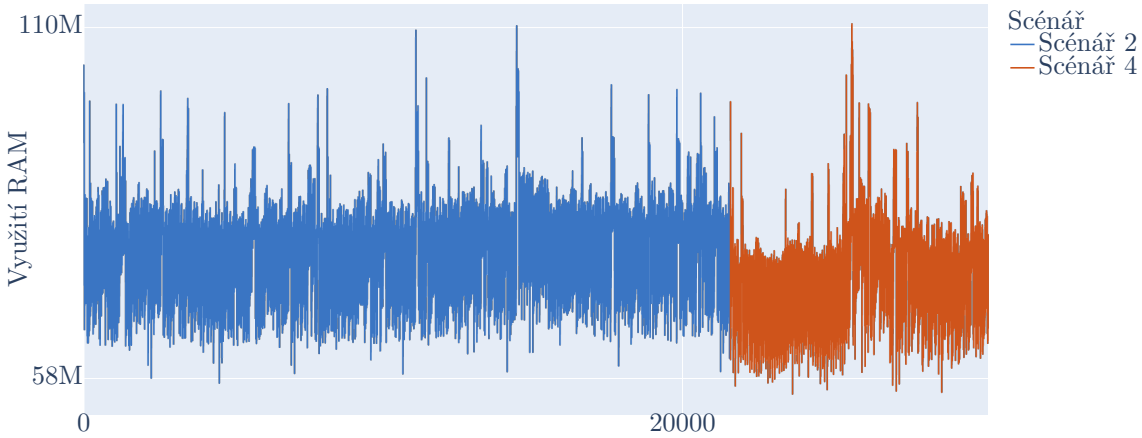
### 6.9.2 Využití systémových prostředků

Oproti 6.7 byl zaznamenán významný pokles spotřeby operační paměti procesem *com.google.android.apps.maps*, pokud jde o počet záznamů. Průměrná spotřeba mírně vzrostla.



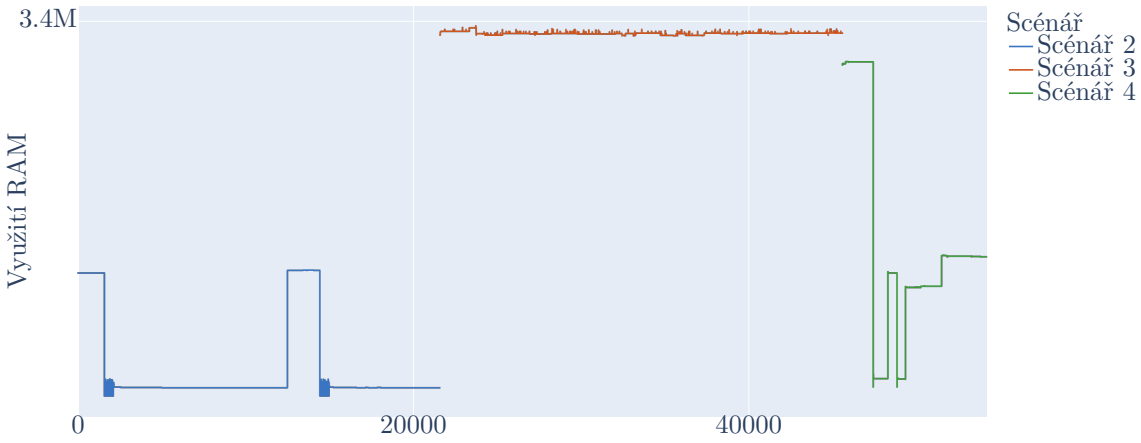

**Obrázek 6.25** Scénáře 2, 4: využití RAM procesem com.google.android.apps.maps

Spotřeba RAM procesem *system* opět zaznamenala pokles k nižším hodnotám.



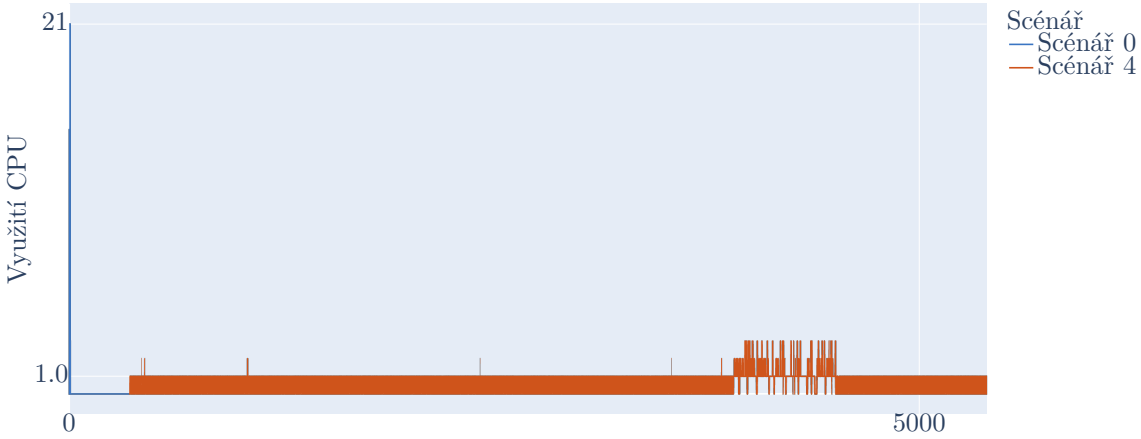

**Obrázek 6.26** Scénáře 2, 4: využití RAM procesem system

U procesu *android.hardware.gnss* byly zaznamenány hodnoty vytížení RAM rozsahem mezi scénáři 6.7 a 6.8, oproti scénáři 6.7 navíc nebyla identifikována periodicita.




**Obrázek 6.27** Scénáře 2-4: využití RAM procesem android.hardware.gnss

Spotřeba procesoru procesem *android.hardware.sensors* sice nenabývala takových hodnot jako u scénáře 6.5, avšak po celou dobu měření bylo u procesu překvapivě zaznamenáváno nenulové vytížení procesoru.




**Obrázek 6.28** Scénáře 0, 4: využití CPU procesem android.hardware.sensors

## 6.10 Scénář 5

Měření tohoto scénáře navázalo na 6.9, změna spočívala v opětovném zapnutí určování polohy.

**Tabulka 6.11** Podmínky scénáře 5

| | |
|---|---|
| Určování polohy | Povoleno |
| Asistent Google Go | Zakázán |
| Hlasové služby od Googlu | Zakázány |
| SIM karta v telefonu | Ano |
| Aplikace na pozadí | Žádné |
| Přibližná doba měření | 30 hodin |

### 6.10.1 Síťová komunikace

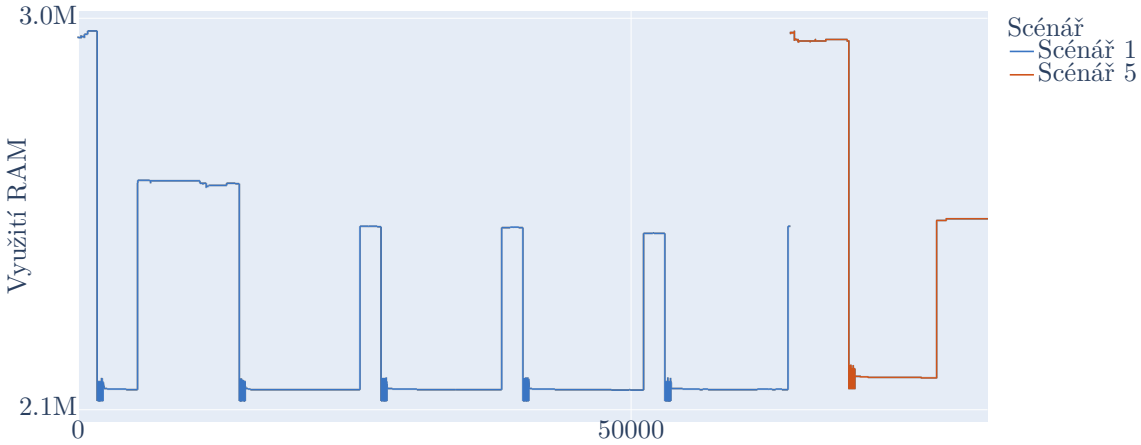
**Tabulka 6.12** Množství bajtů v komunikaci s doménami scénáře 5

| Doména | Odesláno | Přijato | SNIe |
|---|---|---|---|
| 3gppnetwork | 76,8 KB | 19,7 KB | 3,87 KB |
| ad.doubleclick | 55,8 KB | 13,5 KB | 3,16 KB |
| adservices | 82 KB | 21,6 KB | 10 KB |
| googleusercontent | 72,3 KB | 21,3 KB | 549 B |
| mobilemaps | 163 KB | 71,6 KB | 4,94 KB |
| tclclouds, tclcom | 0 B | 0 B | 0 B |
| tct-supportcenter | 31,9 KB | 7,52 KB | 2,74 KB |
| userlocation | 518 KB | 548 KB | 549 B |
| Celkem | 26,03 MB | 3,01 MB | 265 KB |

Doména userlocation.googleapis.com tentokráte sdílí IP adresy s pouze 10 dalšími doménami, čímž by se dalo vysvětlit snížení objemu komunikace směrem z této skupiny domén. Byl zaznamenán pokles komunikace z *mobilemaps*, zároveň také nárůst v objemu dat zaslaných telefonem. Nárůst u *tct-supportcenter* neodpovídá nárůstu doby měření, nicméně nedomnívám se, že jde o podezřelé chování. Překvapivým jevem je vymizení komunikace *tclclouds, tclcom*. Po podrobnějším zkoumání objemu komunikace v jednotlivé dny v týdnu docházím k závěru, že i nárůst *3gppnetwork* je ospravedlnitelný. Dny, které byly měřením zachyceny celé, ukazují, že doména 3gppnetwork.org odešle do telefonu někde mezi 30-40 KB dat a přijme jich mezi 6-10 KB. Množství také závisí na hodinách, ve kterých komunikace probíhá, na této úrovni ovšem nebyl nalezen opakující se vzor. Doména ad.doubleclick.net opět zaznamenala výraznější nárůst odchozí komunikace, avšak nijak zásadní nárůst příchozí komunikace, doména googleusercontent.com zaznamenala výrazný nárůst oběma směry, *adservices* ovšem zaznamenaly pokles napříč prodloužení doby měření.

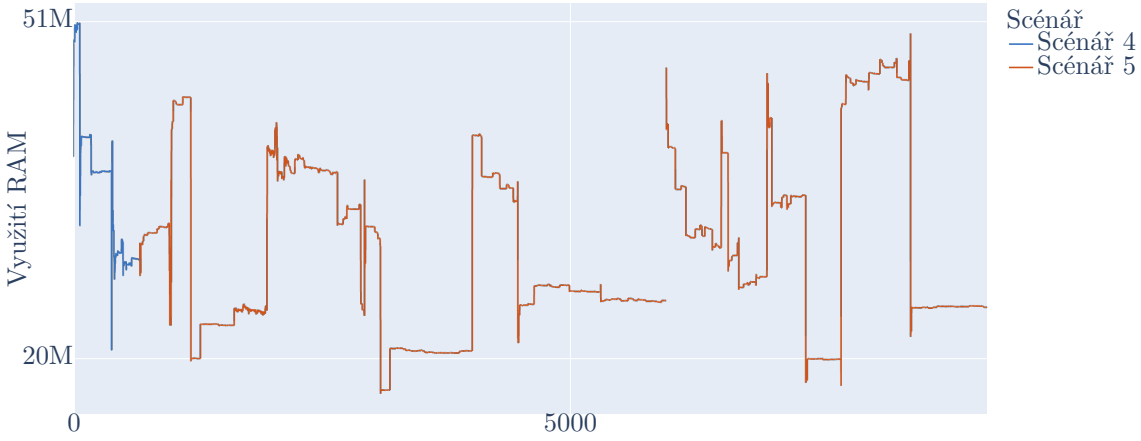
### 6.10.2 Využití systémových prostředků

Ač jsou podmínky scénářů 6.6 a 6.10 protichůdné (v nastavení určování zeměpisné polohy), tak u procesu *android.hardware.gnss* mezi nimi existuje podobnost ve vytížení operační paměti, což se nedá označit jako očekávané chování.



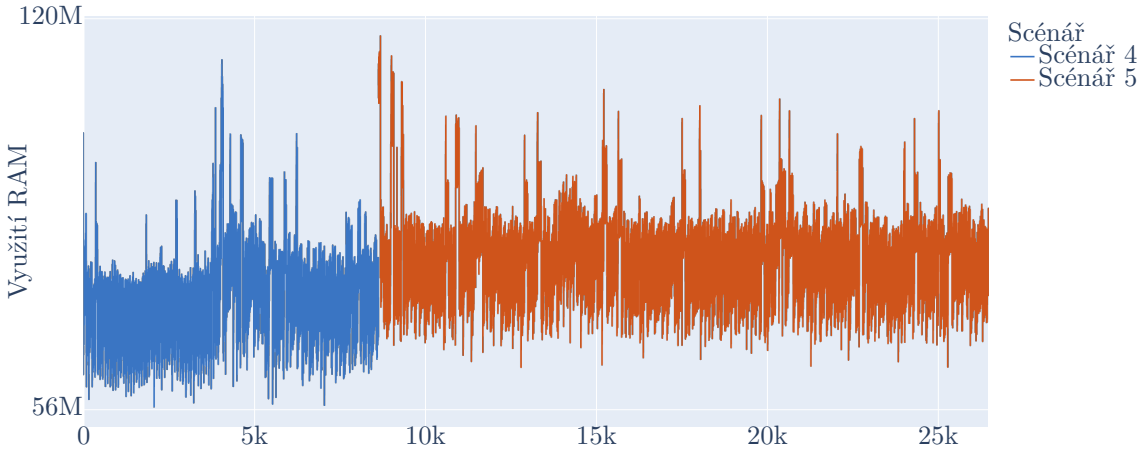

**Obrázek 6.29** Scénáře 1, 5: využití RAM procesem android.hardware.gnss

U *com.google.android.apps.maps* bylo registrováno mnohem více záznamů oproti předchozímu scénáři 6.9, dle očekávání.




**Obrázek 6.30** Scénáře 4, 5: využití RAM procesem com.google.android.apps.maps

Změnu v konfiguraci zaznamenal i proces *system*, když mírně zvýšil vytížení.




**Obrázek 6.31** Scénáře 4, 5: využití RAM procesem system

## 6.11 Scénář 6

Toto měření zkoumá chování telefonu bez SIM karty, když cílí na komunikaci domény 3gppnetwork.org.

**Tabulka 6.13** Podmínky scénáře 6

| | |
|---|---|
| Určování polohy | Povoleno |
| Asistent Google Go | Zakázán |
| Hlasové služby od Googlu | Zakázány |
| SIM karta v telefonu | Ne |
| Běžící aplikace na pozadí | Žádné |
| Přibližná doba měření | 24 hodin |

### 6.11.1 Síťová komunikace

**Tabulka 6.14** Množství bajtů v komunikaci s doménami scénáře 6

| Doména | Odesláno | Přijato | SNIe |
|---|---|---|---|
| 3gppnetwork | 0 B | 0 B | 0 B |
| ad.doubleclick | 28,8 KB | 8,75 KB | 2,51 KB |
| adservices | 75 KB | 24 KB | 4,83 KB |
| googleusercontent | 39,6 KB | 3,64 KB | 0 B |
| mobilemaps | 82,1 KB | 47,2 KB | 2,74 KB |
| tclclouds, tclcom | 13,1 KB | 3,45 KB | 549 B |
| tct-supportcenter | 25,5 KB | 5,95 KB | 2,2 KB |
| userlocation | 544 KB | 668 KB | 549 B |
| Celkem | 6,31 MB | 2,53 MB | 120 KB |

Komunikace odpovídá očekáváním, navíc se skutečně ukázalo, že bez SIM karty se telefon nesnažil komunikovat s *3gppnetwork*.

### 6.11.2 Využití systémových prostředků

Mezi procesy nebylo shledáno žádné zaznamenání hodné chování.

## 6.12 Scénář 7

Toto měření navíc oproti 6.11 pouze zakáže určovat polohu.

**Tabulka 6.15** Podmínky scénáře 7

| | |
|---|---|
| Určování polohy | Zakázáno |
| Asistent Google Go | Zakázán |
| Hlasové služby od Googlu | Zakázány |
| SIM karta v telefonu | Ne |
| Aplikace na pozadí | Žádné |
| Přibližná doba měření | 24 hodin |

### 6.12.1 Síťová komunikace

**Tabulka 6.16** Množství bajtů v komunikaci s doménami scénáře 7

| Doména | Odesláno | Přijato | SNIe |
|---|---|---|---|
| 3gppnetwork | 0 B | 0 B | 0 B |
| ad.doubleclick | 29,5 KB | 8,92 KB | 2,51 KB |
| adservices | 97,5 KB | 25,1 KB | 5,82 KB |
| googleusercontent | 42,2 KB | 12,8 KB | 549 B |
| mobilemaps | 119 KB | 59,6 KB | 3,84 KB |
| tclclouds, tclcom | 13,1 KB | 3,45 KB | 549 B |
| tct-supportcenter | 25,6 KB | 6,04 KB | 2,2 KB |
| userlocation | 680 KB | 617 KB | 549 B |
| Celkem | 3,88 MB | 2,8 MB | 107 KB |

Dle očekávání se opět nevyskytuje komunikace s *3gppnetwork*, zajímavostí je téměř nulová odchylka *tct-supportcenter*, *tclclouds, tclcom* od hodnot z předchozího měření 6.11.1. Jak se zdá, *mobilemaps* nijak nereagují na přítomnost SIM karty v telefonu, nakolik došlo k navýšení komunikace ve všech směrech. Část předchozího výroku o absenci reakce na přítomnost SIM karty v telefonu se dá říct o všech ostatních doménách tabulky 6.16.

### 6.12.2 Využití systémových prostředků

Mezi procesy nebylo shledáno žádné zaznamenání hodné chování.

## 6.13 Scénář 8

Tento scénář se věnuje zaznamenávání aktivity telefonu se zapnutou aplikací Mapy Google na hlavní obrazovce telefonu při pohybu. Doba měření byla relativně krátká kvůli technickým omezením spojených se snímáním vlastností telefonu – bylo potřeba zajistit dostupnost GPS signálu a udržet připojení k Wi-Fi síti, vytvořenou pro potřeby měření, tím i přístup k Internetovému připojení.

**Tabulka 6.17** Podmínky scénáře 8

| | |
|---|---|
| Určování polohy | Povoleno |
| Asistent Google Go | Zakázán |
| Hlasové služby od Googlu | Zakázány |
| SIM karta v telefonu | Ne |
| Aplikace na pozadí | Žádné |
| Mapy Google na popředí | Ano |
| Aktivní pohyb | Ano |
| Přibližná doba měření | 1 hodina |

### 6.13.1 Síťová komunikace

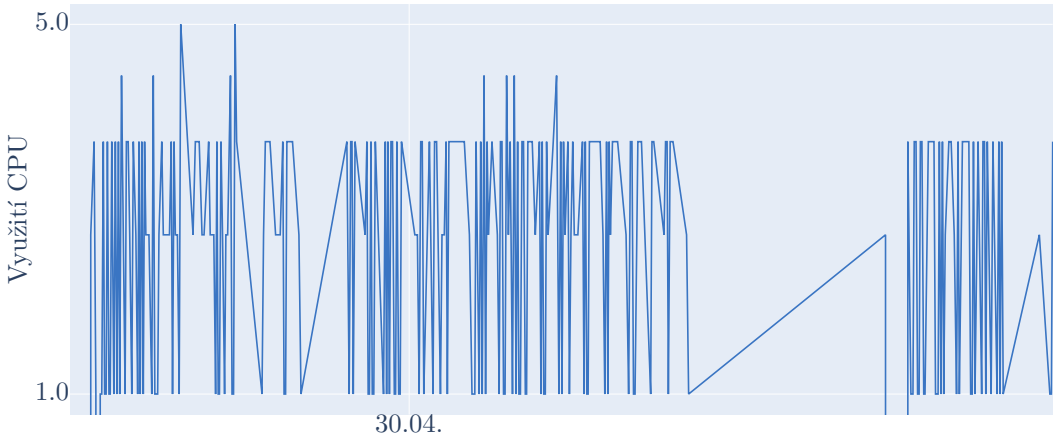
**Tabulka 6.18** Množství bajtů v komunikaci s doménami scénáře 8

| Doména | Odesláno | Přijato | SNIe |
|---|---|---|---|
| 3gppnetwork | 0 B | 0 B | 0 B |
| ad.doubleclick | 0 B | 0 B | 0 B |
| adservices | 0 B | 0 B | 0 B |
| googleusercontent | 0 B | 0 B | 0 B |
| mobilemaps | 450 KB | 256 KB | 8,56 KB |
| tclclouds, tclcom | 0 B | 0 B | 0 B |
| tct-supportcenter | 0 B | 0 B | 0 B |
| userlocation | 0 B | 0 B | 0 B |
| Celkem | 830 KB | 836 KB | 25,8 KB |

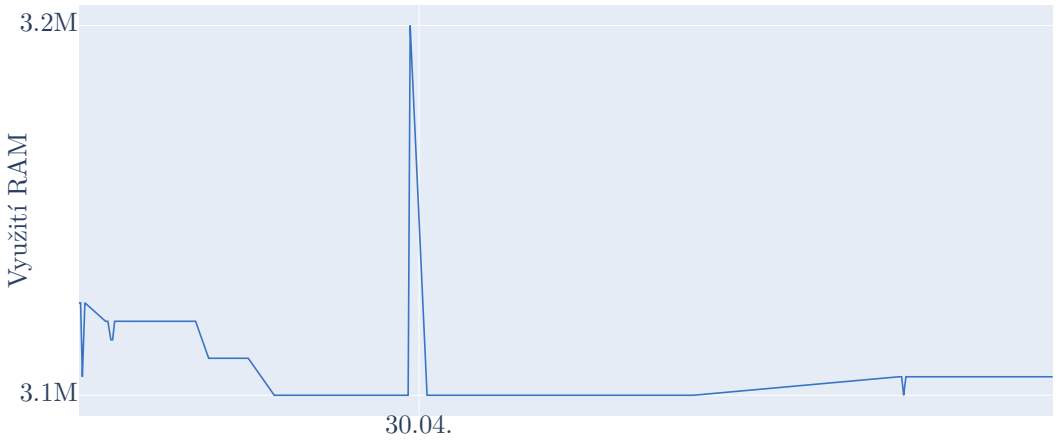
Účelem měření bylo hlavně potvrzení, že *mobilemaps* jsou hlavní doménou pro Mapy Google. Osobně označuju za překvapivý jev nulovou komunikaci *userlocation*. Nulová komunikace ostatních domén lze však, po mém soudu, ospravedlnit příliš krátkou dobou měření.

### 6.13.2 Využití systémových prostředků

Tak jako u scénáře 6.8 i tentokráte byl u spotřeby procesoru výrazně zastoupen proces *android.hardware.gnss*. Spotřeba operační paměti byla velmi blízko hodnotám naměřeným při 6.8.

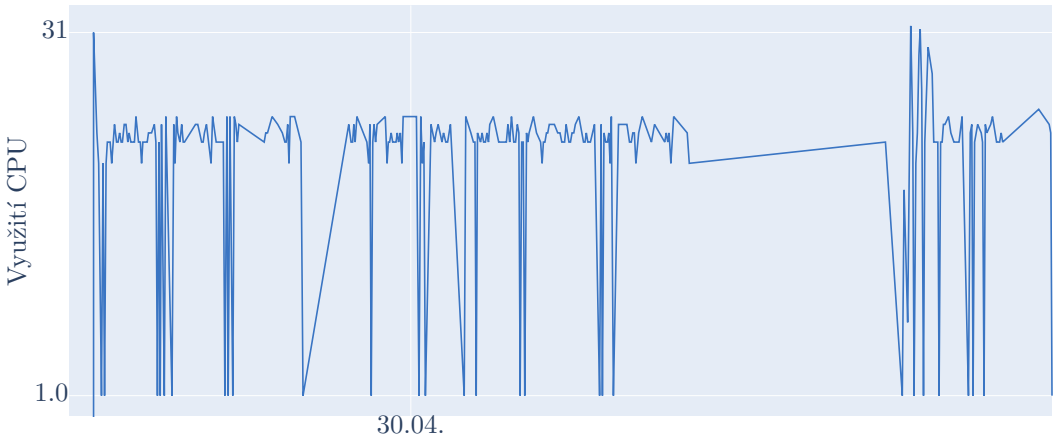



**Obrázek 6.32** Scénář 8: využití CPU procesem android.hardware.gnss

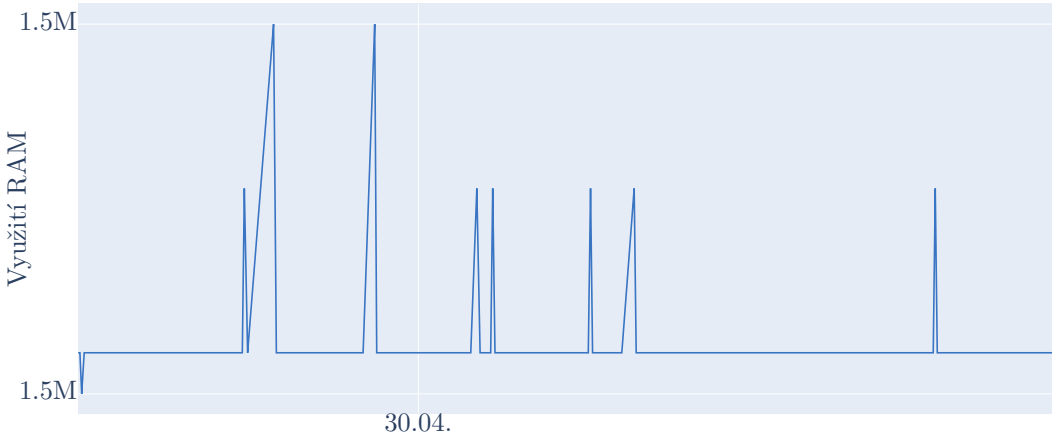



**Obrázek 6.33** Scénář 8: využití RAM procesem android.hardware.gnss

Spotřeba CPU procesem *android.hardware.sensors* byla také výraznější oproti „klidovému“ stavu, totéž se dá říct i o operační paměti.

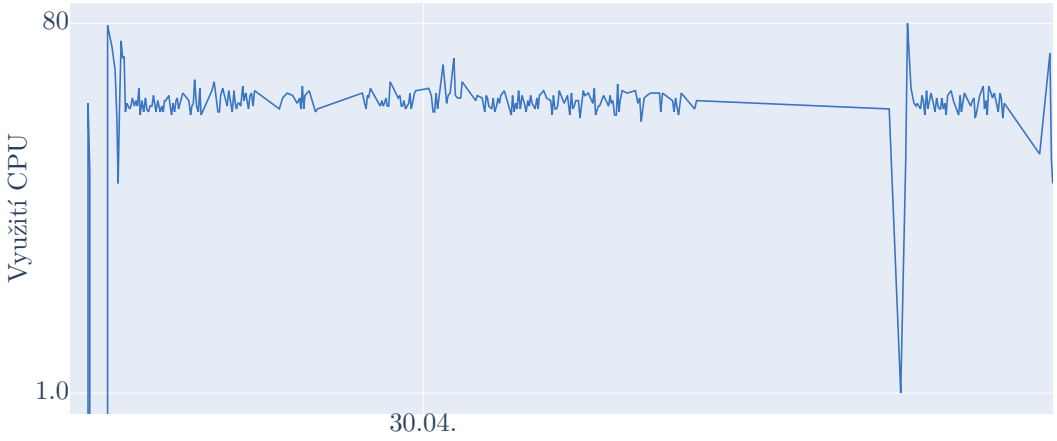



**Obrázek 6.34** Scénář 8: využití CPU procesem android.hardware.sensors




**Obrázek 6.35** Scénář 8: využití RAM procesem android.hardware.sensors

Přikládám i proces *com.google.android.apps.maps*.




**Obrázek 6.36** Scénář 8: využití CPU procesem com.google.android.apps.maps

## 6.14 Scénář 9

Tento scénář opět navazuje na 6.13, jedinou změnou je opětovné zapojení SIM karty.

**Tabulka 6.19** Podmínky scénáře 9

| | |
|---|---|
| Určování polohy | Povoleno |
| Asistent Google Go | Zakázán |
| Hlasové služby od Googlu | Zakázány |
| SIM karta v telefonu | Ano |
| Aplikace na pozadí | Žádné |
| Mapy Google na popředí | Ano |
| Aktivní pohyb | Ano |
| Přibližná doba měření | 1 hodina |

### 6.14.1 Síťová komunikace

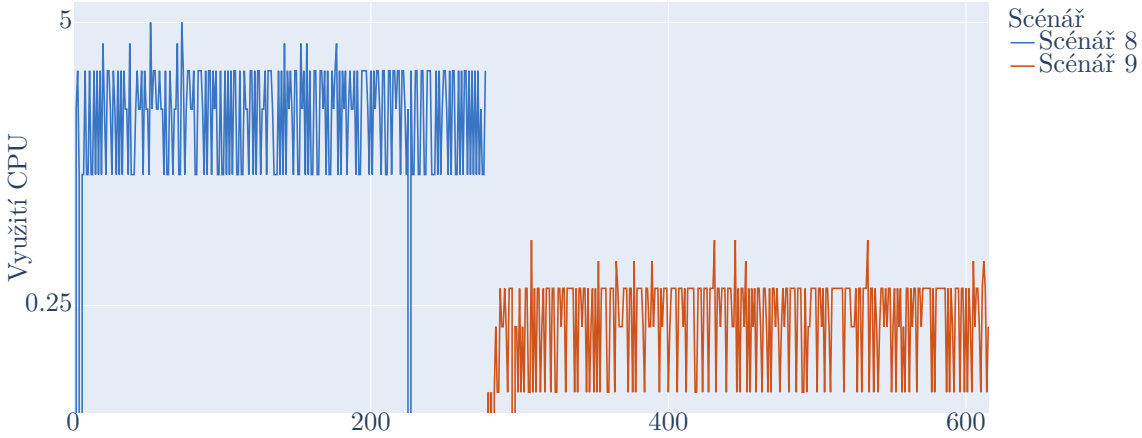
**Tabulka 6.20** Množství bajtů v komunikaci s doménami scénáře 9

| Doména | Odesláno | Přijato | SNIe |
|---|---|---|---|
| 3gppnetwork | 4,83 KB | 1,25 KB | 242 B |
| ad.doubleclick | 0 B | 0 B | 0 B |
| adservices | 0 B | 0 B | 0 B |
| googleusercontent | 89,4 KB | 8,46 KB | 1,65 KB |
| mobilemaps | 2,36 MB | 182 KB | 5,48 KB |
| tclclouds, tclcom | 0 B | 0 B | 0 B |
| tct-supportcenter | 0 B | 0 B | 0 B |
| userlocation | 0 B | 0 B | 0 B |
| Celkem | 3,37 MB | 930 KB | 26,8 KB |

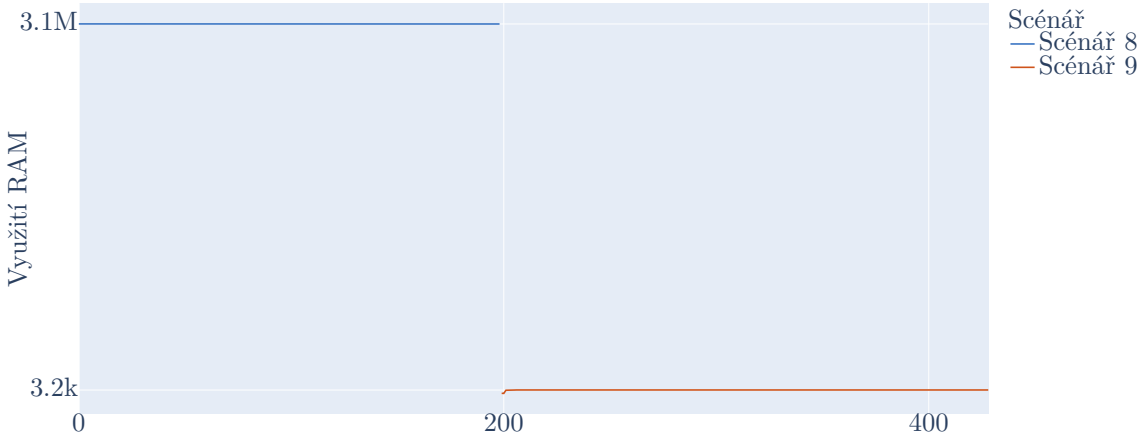
Je vidět, že opět probíhala komunikace s *3gppnetwork*, zatímco komunikace *mobilemaps* výrazně narostla oproti předchozímu scénáři. Nicméně myslím si, že se to dá v tomto případě označit za očekávané.

### 6.14.2 Využití systémových prostředků

Přijde mi neočekávané, nikoliv nežádoucí, řádové snížení spotřeby procesoru procesem *android.hardware.gnss* oproti předchozímu měření. V souladu s tím byla řádově nižší i spotřeba operační paměti.

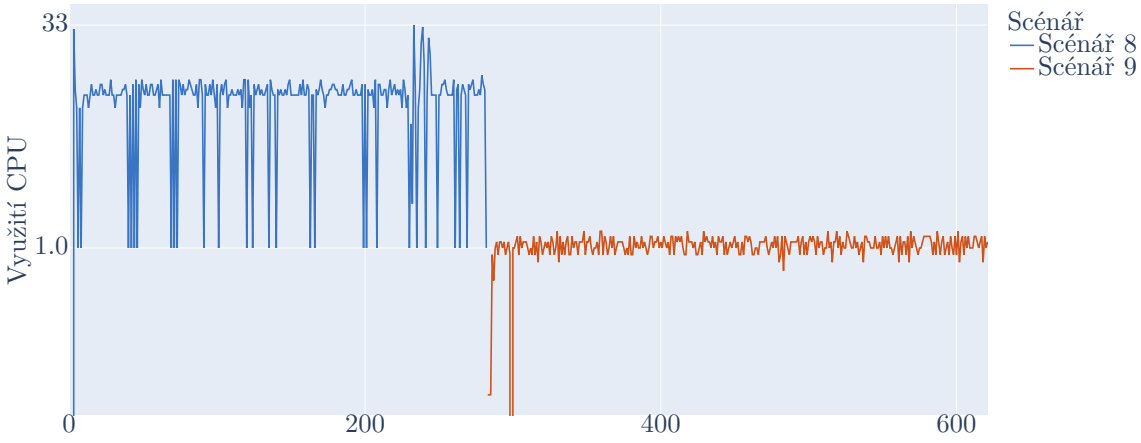



**Obrázek 6.37** Scénáře 8, 9: využití CPU procesem android.hardware.gnss



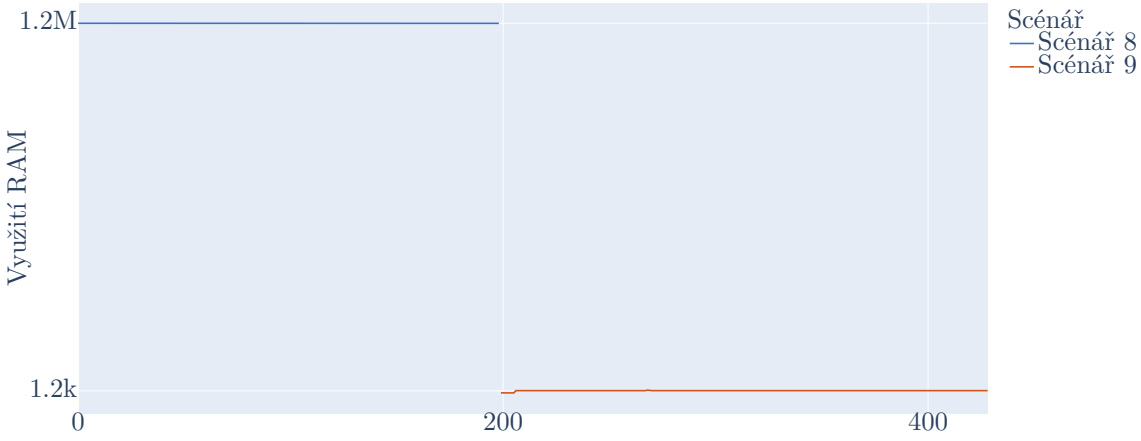

**Obrázek 6.38** Scénáře 8, 9: využití RAM procesem android.hardware.gnss

Dokonce i proces *android.hardware.sensors* registroval řádový pokles vytížení operační paměti.



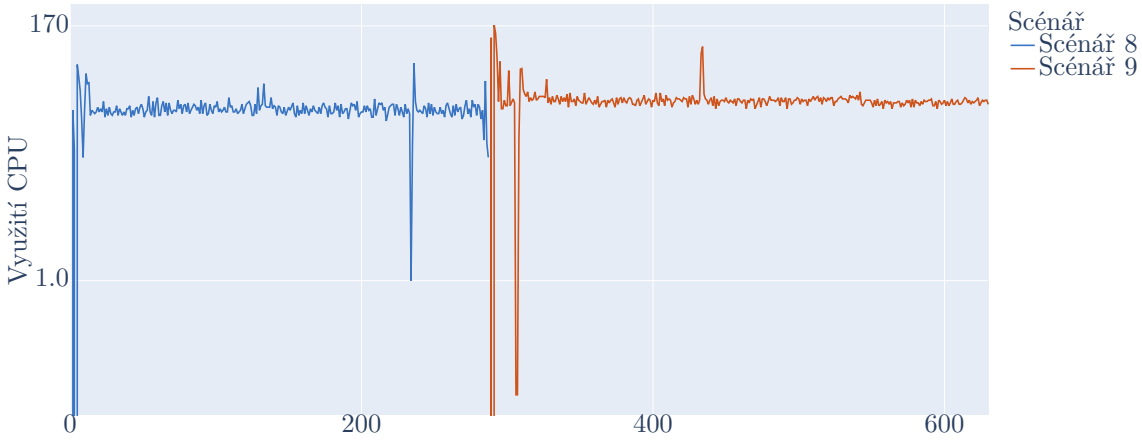

**Obrázek 6.39** Scénáře 8, 9: využití RAM procesem android.hardware.sensors

Poslední překvapivé poznání tohoto měření je, že i proces *android.hardware.wifi* využíval RAM výrazně méně.




**Obrázek 6.40** Scénáře 8, 9: využití RAM procesem android.hardware.wifi

Spotřeba procesoru *com.google.android.apps.maps* se držela na podobné, o trošku vyšší, úrovni.




**Obrázek 6.41** Scénáře 8, 9: využití CPU procesem com.google.android.apps.maps

## 6.15 Scénář 10

Tento scénář si kladl za cíl prozkoumat, zda se ovlivní nabízené reklamy při probíhající konverzaci o produktech, což by znamenalo přítomnost odposlechu uživatelů. Pro detekci byla zvolena metoda přehrávaného zvuku mp3 souborů extrahovaných z různých recenzních videí.

**Tabulka 6.21** Podmínky scénáře 10

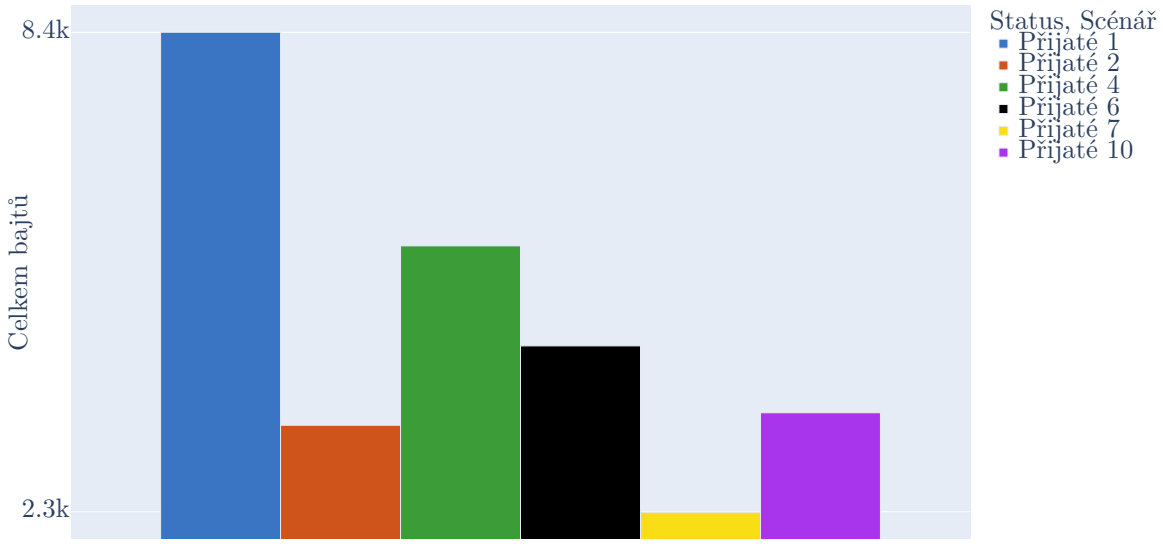
| | |
|---|---|
| Určování polohy | Povoleno |
| Asistent Google Go | Zakázán |
| Hlasové služby od Googlu | Povoleny |
| SIM karta v telefonu | Ano |
| Aplikace na pozadí | Žádné |
| Přibližná doba měření | 2 hodiny |

### 6.15.1 Síťová komunikace

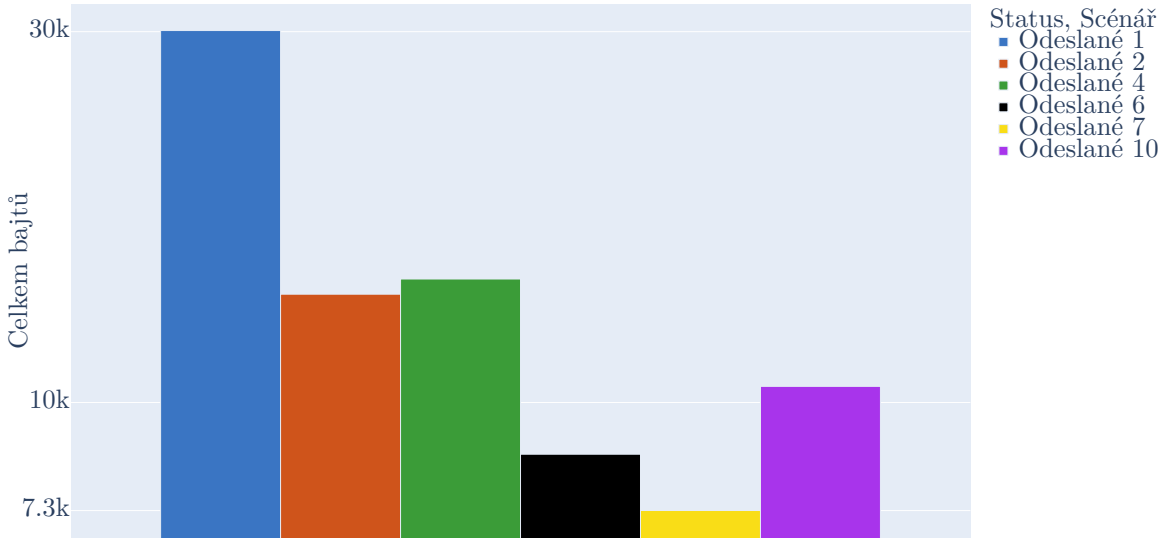
**Tabulka 6.22** Množství bajtů v komunikaci s doménami scénáře 10

| Doména | Odesláno | Přijato | SNIe |
|---|---|---|---|
| 3gppnetwork | 0 B | 0 B | 0 B |
| ad.doubleclick | 19,8 KB | 5,94 KB | 981 B |
| adservices | 34,3 KB | 20,4 KB B | 2,53 KB |
| googleusercontent | 0 B | 0 B | 0 B |
| mobilemaps | 0 B | 0 B | 0 B |
| tclclouds, tclcom | 0 B | 0 B | 0 B |
| tct-supportcenter | 0 B | 0 B | 0 B |
| userlocation | 0 B | 0 B | 0 B |
| Celkem | 28,5 MB | 1,04 MB | 37,6 KB |

Musím konstatovat, že se po konci měření nijak nezměnily nabízené reklamy. Nasvědčuje tomu i objem komunikace *ad.doubleclick*. Na první pohled je zde sice nad očekávání vysoká komunikace, jenomže detailnější analýza mezi scénáři dokazuje, že polovina dat byla odeslána mezi 19. a 20. hodinou, což je čas, ve kterém probíhala komunikace s doménou vůbec nejčastěji, napříč mezi až dosud vykonanými, často protichůdnými scénáři. *adservices* registrovaly obdobný jev, leč kvůli nízké čitelnosti graf neuvádím.




**Obrázek 6.42** Scénáře 1, 2, 4, 6, 7, 10: agregovaná příchozí komunikace ad.doubleclick.net mezi 19. až 20. hodinou




**Obrázek 6.43** Scénáře 1, 2, 4, 6, 7, 10: agregovaná odchozí komunikace ad.doubleclick.net mezi 19. až 20. hodinou

### 6.15.2 Využití systémových prostředků

Ve vytížení systémových prostředků jednotlivých procesů nebyly zjištěny žádné zaznamenání hodné informace.

## 6.16 Scénář 11

Tento scénář navazuje na 6.15. Hlavní rozdíl, mimo délky měření, spočívá v tom, že byl zaměřen na rozpoznání „živého“ lidského hlasu, tedy bez použití mp3 záznamů.

**Tabulka 6.23** Podmínky scénáře 11

| | |
|---|---|
| Určování polohy | Povoleno |
| Asistent Google Go | Zakázán |
| Hlasové služby od Googlu | Povoleny |
| SIM karta v telefonu | Ano |
| Aplikace na pozadí | Žádné |
| Přibližná doba měření | 35 hodin |

### 6.16.1 Síťová komunikace

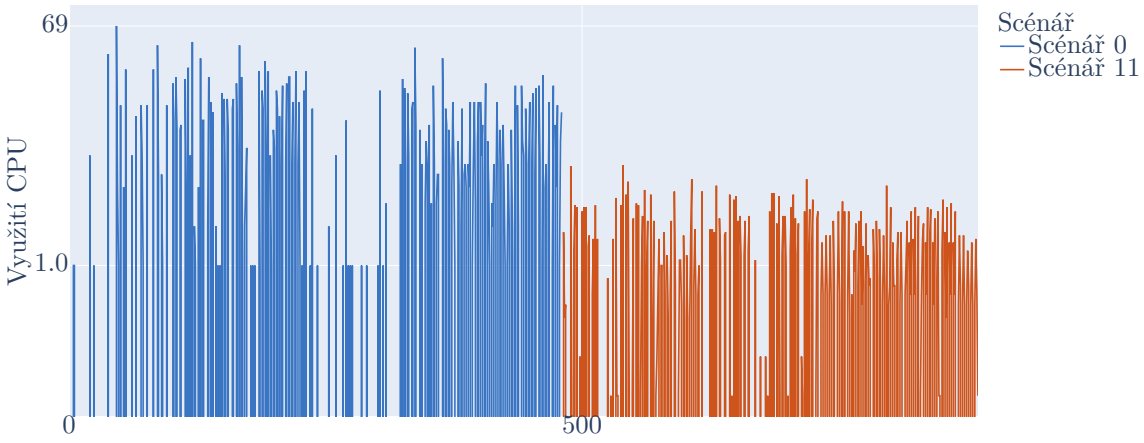
**Tabulka 6.24** Množství bajtů v komunikaci s doménami scénáře 11

| Doména | Odesláno | Přijato | SNIe |
|---|---|---|---|
| 3gppnetwork | 38,2 KB | 13,2 KB | 1,94 KB |
| ad.doubleclick | 36,5 KB | 10,5 KB | 2,73 KB |
| adservices | 133 KB | 54,9 KB | 8,24 KB |
| googleusercontent | 89,2 KB | 23,4 KB | 0 B |
| mobilemaps | 172 KB | 95,6 KB | 5,49 KB |
| tclclouds, tclcom | 13,4 KB | 3,45 KB | 549 B |
| tct-supportcenter | 38,7 KB | 8,97 KB | 3,29 KB |
| userlocation | 1,51 MB | 1,59 MB | 549 B |
| Celkem | 21,2 MB | 5,76 MB | 199 KB |

Konstatuji, že změna nabízených reklam se neudála ani nyní, zároveň nebyl zaznamenán neobvyklý objem komunikace na žádném z výše zmíněných záznamů.

### 6.16.2 Využití systémových prostředků

Jediný proces, který stojí za zmínku je *com.google.android.tts*. Ten byl nástrojem cpuinfo spatřován podobně často jako při úvodním měření, avšak v tomto případě jeho průměrná spotřeba nedosahovala ani 1 %.




**Obrázek 6.44** Scénáře 0, 11: využití CPU procesem com.google.android.tts

## 6.17 Scénář 12

Tento scénář navazuje svými vlastnostmi na scénář 6.9. Je zde přes aplikaci Nastavení explicitně ukončena aplikace Mapy Google. Cílem je prozkoumat aktivitu související zejména s touto aplikací.

**Tabulka 6.25** Podmínky scénáře 12

| | |
|---|---|
| Určování polohy | Povoleno |
| Asistent Google Go | Zakázán |
| Hlasové služby od Googlu | Povoleny |
| SIM karta v telefonu | Ano |
| Aplikace na pozadí | Žádné |
| Přibližná doba měření | 24 hodin |

### 6.17.1 Síťová komunikace

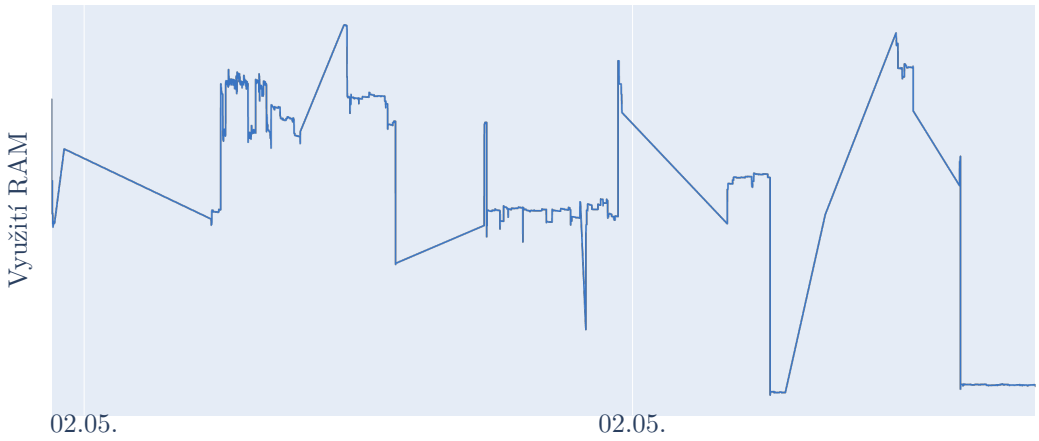
**Tabulka 6.26** Množství bajtů v komunikaci s doménami scénáře 12

| Doména | Odesláno | Přijato | SNIe |
|---|---|---|---|
| 3gppnetwork | 52,8 KB | 13,5 KB | 2,66 KB |
| ad.doubleclick | 49,9 KB | 12,1 KB | 2,61 KB |
| adservices | 132 KB | 43,5 KB | 8,02 KB |
| googleusercontent | 43,9 KB | 14,3 KB | 549 B |
| mobilemaps | 87,4 KB | 32,4 KB | 2,74 KB |
| tclclouds, tclcom | 13 KB | 3,42 KB | 549 B |
| tct-supportcenter | 32 KB | 7,55 KB | 2,74 KB |
| userlocation | 1,25 MB | 921 KB | 549 B |
| Celkem | 71,7 MB | 4,88 MB | 151 KB |

I přes explicitní ukončení aplikace zde stále překvapivě probíhá komunikace s *mobilemaps*. Rovněž bylo zaznamenáno spojení s *userlocation*.

### 6.17.2 Využití systémových prostředků

Skutečně i přes explicitní ukončení stále existoval proces *com.google.android.apps.maps*.




**Obrázek 6.45** Scénář 12: využití RAM procesem com.google.android.apps.maps

## 6.18 Scénář 13

Oproti předchozímu scénáři 6.17 zde byla změna pouze v přítomnosti SIM karty v telefonu – v tomto scénáři byla vyjmuta.

**Tabulka 6.27** Podmínky scénáře 13

| | |
|---|---|
| Určování polohy | Povoleno |
| Asistent Google Go | Zakázán |
| Hlasové služby od Googlu | Povoleny |
| SIM karta v telefonu | Ne |
| Aplikace na pozadí | Žádné |
| Přibližná doba měření | 24 hodin |

### 6.18.1 Síťová komunikace

**Tabulka 6.28** Množství bajtů v komunikaci s doménami scénáře 13

| Doména | Odesláno | Přijato | SNIe |
|---|---|---|---|
| 3gppnetwork | 0 B | 0 B | 0 B |
| ad.doubleclick | 43,9 KB | 13,6 KB | 4,04 KB |
| adservices | 146 KB | 30 KB | 8,14 KB |
| googleusercontent | 34,6 KB | 4,86 KB | 0 B |
| mobilemaps | 36,7 KB | 12 KB | 1,1 KB |
| tclclouds, tclcom | 13,1 KB | 3,51 KB | 549 B |
| tct-supportcenter | 31,9 KB | 7,46 KB | 2,74 KB |
| userlocation | 14,3 MB | 2,44 MB | 549 B |
| Celkem | 57,8 MB | 3,64 MB | 140 KB |

Zde je ještě jednou potvrzeno, že komunikace s *3gppnetwork* se bez SIM karty skutečně nevyskytuje. Komunikace zbylých domén je dle očekávání.

### 6.18.2 Využití systémových prostředků

Dle očekávání byl i zde zjištěn výskyt procesu *com.google.android.apps.maps*, avšak oproti 6.17.2 by graf nepřinesl nic nového. Grafy vytíženosti zbylých procesů nepřinášejí žádnou novou informaci, proto ani je zde také neuvádím.

## 6.19 Scénář 14

V tomto scénáři byla zkoumána role dostupných Wi-Fi sítí v určování polohy. V telefonu bylo povoleno zjišťování dostupných Wi-Fi sítí za účelem zpřesnění zeměpisné polohy zařízení. Pro potřeby měření bylo jednorázově vygenerováno celkem 250 různých Wi-Fi sítí, 122 z nich ve 2,4GHz frekvenčním pásmu a zbylých 128 v 5GHz pásmu.

**Tabulka 6.29** Podmínky scénáře 14

| | |
|---|---|
| Určování polohy | Povoleno |
| Určování polohy dle Wi-Fi | Povoleno |
| Generování Wi-Fi sítí | Ano |
| Asistent Google Go | Zakázán |
| Hlasové služby od Googlu | Povoleny |
| SIM karta v telefonu | Ano |
| Aplikace na pozadí | Žádné |
| Přibližná doba měření | 26 hodin |

### 6.19.1 Síťová komunikace

**Tabulka 6.30** Množství bajtů v komunikaci s doménami scénáře 14

| Doména | Odesláno | Přijato | SNIe |
|---|---|---|---|
| 3gppnetwork | 43,2 KB | 14,8 KB | 2,18 KB |
| ad.doubleclick | 42 KB | 10,3 KB | 2,39 KB |
| adservices | 63 KB | 17,2 KB | 6,04 KB |
| googleusercontent | 19,7 KB | 4,89 KB | 549 B |
| mobilemaps | 113 KB | 59,4 KB | 3,84 KB |
| tclclouds, tclcom | 13,2 KB | 3,51 KB | 549 B |
| tct-supportcenter | 32 KB | 7,53 KB | 2,74 KB |
| userlocation | 1,45 MB | 1,37 MB | 549 B |
| Celkem | 89,5 MB | 4,21 MB | 158 KB |

Z hlediska síťového provozu nebylo zaznamenáno žádné zvláštní chování.

### 6.19.2 Využití systémových prostředků

K mému překvapení nebyla zaznamenána změna od standardního chování při nultém měření od žádného ze sledovaných procesů. Grafy zde tedy neuvádím, jelikož by nepřinesly žádnou novou informaci.

## 6.20 Scénář 15

Rozdíl tohoto a předchozího scénáře 6.19 tkví v zákazu využití Wi-Fi sítí pro zvýšení přesnosti při určování zeměpisné polohy.

**Tabulka 6.31** Podmínky scénáře 15

| | |
|---|---|
| Určování polohy | Povoleno |
| Určování polohy dle Wi-Fi | Zakázáno |
| Generování Wi-Fi sítí | Ano |
| Asistent Google Go | Zakázán |
| Hlasové služby od Googlu | Povoleny |
| SIM karta v telefonu | Ano |
| Aplikace na pozadí | Žádné |
| Přibližná doba měření | 27 hodin |

### 6.20.1 Síťová komunikace

**Tabulka 6.32** Množství bajtů v komunikaci s doménami scénáře 15

| Doména | Odesláno | Přijato | SNIe |
|---|---|---|---|
| 3gppnetwork | 33,5 KB | 11,3 KB | 1,69 KB |
| ad.doubleclick | 22,2 KB | 6,66 KB | 1,75 KB |
| adservices | 48,6 KB | 14,2 KB | 5,38 KB |
| googleusercontent | 17,4 KB | 4,34 KB | 549 B |
| mobilemaps | 160 KB | 71,2 KB | 4,94 KB |
| tclclouds, tclcom | 13,2 KB | 3,57 KB | 549 B |
| tct-supportcenter | 25,6 KB | 6,03 KB | 2,2 KB |
| userlocation | 1,61 MB | 1,16 MB | 549 B |
| Celkem | 17,3 MB | 4,73 MB | 153 KB |

Komunikace se sledovanými doménami ani v tomto scénáři nedoznala žádných závratných vychýlení.

### 6.20.2 Využití systémových prostředků

Data udávající změny ve využití systémových prostředků zůstala téměř totožná v porovnání s předchozím scénářem.

## 6.21 Scénář 16

Scénář navazuje na 6.19 a 6.20, jelikož se z nich zdá, že nedošlo k zapojení Wi-Fi do zpřesňování zeměpisné polohy. Tentokráte nedojde k jednorázovému vygenerování Wi-Fi sítí, nýbrž periodicky každé 2 minuty se mažou a znova vytváří.

**Tabulka 6.33** Podmínky scénáře 16

| | |
|---|---|
| Určování polohy | Povoleno |
| Určování polohy dle Wi-Fi | Povoleno |
| Generování Wi-Fi sítí | Ano |
| Asistent Google Go | Zakázán |
| Hlasové služby od Googlu | Povoleny |
| SIM karta v telefonu | Ano |
| Aplikace na pozadí | Žádné |
| Přibližná doba měření | 2.5 hodiny |

### 6.21.1 Síťová komunikace

**Tabulka 6.34** Množství bajtů v komunikaci s doménami scénáře 16

| Doména | Odesláno | Přijato | SNIe |
|---|---|---|---|
| 3gppnetwork | 0 B | 0 B | 0 B |
| ad.doubleclick | 1,27 KB | 1,27 KB | 549 B |
| adservices | 2,74 KB | 3,26 KB | 1,1 KB |
| googleusercontent | 0 B | 0 B | 0 B |
| mobilemaps | 0 B | 0 B | 0 B |
| tclclouds, tclcom | 0 B | 0 B | 0 B |
| tct-supportcenter | 0 B | 0 B | 0 B |
| userlocation | 0 B | 0 B | 0 B |
| Celkem | 331 KB | 672 KB | 0 B |

V důsledku krátké doby měření (a také nulového výskytu neočekávaných jevů) se síťová komunikace jeví zcela zbytečná.

### 6.21.2 Využití systémových prostředků

Jelikož počet záznamů koresponduje s dobou měření, grafy by byly značně vychýlené v neprospěch tohoto scénáře, proto zde jen zmíním, že procesy *android.hardware.wifi*, *android.hardware.gnss* a *android.hardware.sensors* proti očekávání zaznamenaly aktivitu na spodní hranici mezi všemi scénáři. Jediný proces, který zaznamenal vyšší spotřebu, na horní hranici mezi scénáři, je *wificond*.

## 6.22 Scénář 17

Jediná změna oproti 6.21 spočívá v zákazu role Wi-Fi sítí při určování zeměpisné polohy.

**Tabulka 6.35** Podmínky scénáře 17

| | |
|---|---|
| Určování polohy | Povoleno |
| Určování polohy dle Wi-Fi | Zakázáno |
| Generování Wi-Fi sítí | Ano |
| Asistent Google Go | Zakázán |
| Hlasové služby od Googlu | Povoleny |
| SIM karta v telefonu | Ano |
| Aplikace na pozadí | Žádné |
| Přibližná doba měření | 2.5 hodiny |

### 6.22.1 Síťová komunikace

**Tabulka 6.36** Množství bajtů v komunikaci s doménami scénáře 17

| Doména | Odesláno | Přijato | SNIe |
|---|---|---|---|
| 3gppnetwork | 0 B | 0 B | 0 B |
| ad.doubleclick | 7,16 KB | 2,37 KB | 765 B |
| adservices | 14,3 KB | 6,06 KB | 989 B |
| googleusercontent | 0 B | 0 B | 0 B |
| mobilemaps | 17,6 KB | 6,05 KB | 0 B |
| tclclouds, tclcom | 0 B | 0 B | 0 B |
| tct-supportcenter | 6,36 KB | 1,48 KB | 549 B |
| userlocation | 0 B | 0 B | 0 B |
| Celkem | 508 KB | 342 KB | 12,3 KB |

Síťový provoz zde byl o něco bohatší, nicméně na základě již provedených měření se nedomnívám, že se událo cokoli překvapivého.

### 6.22.2 Využití systémových prostředků

Výsledky z hlediska využití systémových prostředků jsem prakticky totožné s 6.21.2.

## 6.23 Diskuse výsledků

Jak udává například Tabulka 6.37 zkoumající korelaci (míru lineární závislosti veličin, jejíž hodnoty pochází z intervalu $\langle -1; 1 \rangle$), *3gppnetwork*, *ad.doubleclick*, *adservices* společně s *tct-supportcenter* se chovaly poměrně očekávaně vzhledem k délce měření jednotlivých scénářů. Jelikož účel bakalářské práce nebyl zkoumat obsah odesílaných dat, je obtížné určit rizikovost komunikace s vyjmenovanými doménami pouze na základě informací o doménách nebo objemu přenesených dat. V souladu s tím, že jsem nezaznamenal například žádnou změnu v nabízených reklamách na základě odposlechu, se nepřikláním k tvrzení, že tyto domény představují velké riziko z hlediska narušení uživatelova soukromí. U *3gppnetwork* byla navíc zjištěna spojitost s přítomností SIM karty v telefonu, komunikace s doménou neprobíhá, pokud je SIM karta z telefonu vyjmuta, což je očekávaný jev.

Pokud jde o *tclclouds, tclcom* tak zde korelační koeficient není až tak významný (důsledek 6.5), během úvodního měření byl zaznamenán abnormálně vysoký přenos dat, který se ale v dalších scénářích nevyskytl. Ač komunikace v některých měřeních nebyla vůbec zaznamenána, tak vzhledem k nízkému rozsahu hodnot „nenulových komunikací“ a k faktu, že jsem nezaznamenal reakci na změny v telefonu, se domnívám, že ani tato doména nepředstavuje přílišné riziko.

Bylo pro mě překvapením, že komunikace *mobilemaps* probíhala nezávisle na nastavení oprávnění zeměpisné polohy nebo na tom, zda je zapnutá aplikace Mapy Google. V těchto případech byla rovněž zaznamenána spotřeba operační paměti procesem *com.google.android.apps.maps*. Je možné, že se proces v paměti udržuje, aby se například uživatel nemusel po každém otevření aplikace znovu přihlásit. Tomuto by nahrával i fakt, že významná aktivita ve vytížení procesoru byla zaznamenána jen v případech, kdy Mapy Google běžely na hlavní obrazovce, avšak, ač ne příliš frekventované, nenulové vytížení procesoru bylo zjištěno téměř ve všech měřeních. Poněkud překvapivě probíhala komunikace s *userlocation* podle specifikovaného atributu SNIe i při zakázaném určování zeměpisné polohy. V konečném důsledku tedy považuji chování spojené, zejména s těmito doménami, za podezřelé, překvapivé a neočekávané.

**Tabulka 6.37** Korelační koeficienty mezi objemem doménou přenesených dat a délkou měření.

| Doména | Odesláno | Přijato |
|---|---|---|
| 3gppnetwork | 0.86 | 0.85 |
| ad.doubleclick | 0.95 | 0.93 |
| adservices | 0.95 | 0.93 |
| tclclouds, tclcom | 0.44 | 0.45 |
| tct-supportcenter | 0.99 | 0.97 |

Spotřeba procesoru procesy *android.hardware.sensors*, *android.hardware.gnss* a *xtra-daemon* udržovala vyšší hodnoty pouze během měření v nichž byla spuštěna aplikace Mapy Google na hlavní obrazovce (scénáře 6.8 a 6.13), což označuji za očekávané chování. Mimo tyto scénáře chování procesů vykazovalo podobné charakteristiky. Pro vytížení operační paměti se dá říct to samé.

Zvýšená spotřeba operační paměti procesem *android.hardware.wifi* byla registrována při měřeních 6.8 a 6.13, zvýšená spotřeba operační paměti byla navíc identifikována ve scénáři 6.15, v němž se zkoumal odposlech uživatelů. Spotřeba prostředků u *wificond* byla zvýšena pouze u scénáře 6.8. Tato zjištění považuji za očekávaná.

Konstatuji, že se nepovedla identifikovat aktivita spojená s monitorováním okolních Wi-Fi sítí. Myslím si, že odůvodnění mohou být některá z následujících:

- krátká doba měření,
- příliš malý počet Wi-Fi sítí, ten jsem ovšem nebyl v důsledku technických omezení schopen navýšit,

- příliš široký interval, v němž došlo k „regeneraci“ sítí,
- aktivita vůbec neprobíhala.

# Kapitola 7
# Závěr

Cílem práce bylo ověření hypotézy *„mobilní telefony s operačním systémem Android mohou být zneužity pro sledování uživatelů bez jejich vědomí.“* Data využitá k vyhodnocení hypotézy pochází ze síťové komunikace mobilního telefonu i ze statistik ohledně jeho vytížení procesoru a operační paměti. Dle zadání jsem měl postupovat inkrementálním způsobem, tedy nejprve na mobilním telefonu v továrním nastavení a poté s nainstalovanými potenciálně škodlivými aplikacemi. Vzhledem k velké časové náročnosti měření byl zkoumán pouze mobilní telefon v továrním nastavení. Nad rámec zadání byla také vytvořena webová aplikace, jež je určena pouze pro lokální práci. Tato aplikace umožňuje selekci dat vykreslených do grafů, přičemž s nimi také umožňuje interaktivní manipulaci.

Byla zjištěna podezřelá aktivita zejména procesu aplikace Mapy Google a komunikace domén, které by podle omezeného množství dostupných informací měly umožňovat fungování této aplikace. Nebyla zjištěna aktivita spojená s určováním polohy pomocí výskytu okolních Wi-Fi sítí ani nebyl detekován uživatelský odposlech. Zjištěná aktivita neumožňuje tvrdit, že dochází k nežádoucímu chování, avšak v souladu se zadáním a výsledky měření lze tvrdit, že k němu může docházet, na základě výsledků měření výlučně prostřednictvím mapové aplikace a mapových domén.

Do budoucna by šlo na práci navázat rozšířením scénářů, hlavně pokud jde o instalaci dalších aplikací, stejně jako prodloužením doby měření, ideálně řádově na týdny. Šlo by rozšířit i webovou aplikaci například o implementaci statistických metod nebo obecněji rozšířením možností filtrování dat.

# Příloha A

# Vzhled webové aplikace


**Obrázek A.1** Vzhled části aplikace pracující s daty využití systémových prostředků


**Obrázek A.2** Vzhled části aplikace pracující s daty síťového provozu

# Bibliografie


1. GOODWIN, Richard. The History of Mobile Phones From 1973 To 2008: The Cellphones That Made It ALL Happen. *KnowYourMobile* [online]. 2021 [cit. 2022-04-24]. Dostupné z: `https://www.knowyourmobile.com/phones/the-history-of-mobile-phones-from-1973-to-2008-the-handsets-that-made-it-all-happen-d58/`.
2. KEMP, Simon. DIGITAL 2022: GLOBAL OVERVIEW REPORT. *DataReportal – Global Digital Insights* [online]. 2022 [cit. 2022-04-24]. Dostupné z: `https://datareportal.com/reports/digital-2022-global-overview-report`.
3. HAN, Weili; CAO, Chang; CHEN, Hao; LI, Dong; FANG, Zheran; XU, Wenyuan; WANG, X. Sean. senDroid: Auditing Sensor Access in Android System-Wide. *IEEE Transactions on Dependable and Secure Computing*. 2020, roč. 17, č. 2, s. 407–421. Dostupné z DOI: `10.1109/TDSC.2017.2768536`.
4. SIVAN, Nir; BITTON, Ron; SHABTAI, Asaf. Analysis of Location Data Leakage in the Internet Traffic of Android-based Mobile Devices. In: *22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2019)*. Chaoyang District, Beijing: USENIX Association, 2019, s. 243–260. ISBN 978-1-939133-07-6. Dostupné také z: `https://www.usenix.org/conference/raid2019/presentation/sivan`.
5. LI, Fenghua; WANG, Xinyu; NIU, Ben; LI, Hui; LI, Chao; CHEN, Lihua. Exploiting location-related behaviors without the GPS data on smartphones. *Information Sciences*. 2020, roč. 527, s. 444–459. ISSN 0020-0255. Dostupné z DOI: `https://doi.org/10.1016/j.ins.2019.05.052`.
6. VERHEYDEN, Tim; BAERT, Denny; HEE, Lente Van; HEUVEL, Ruben Van Den. Google employees are eavesdropping, even in your living room, VRT NWS has discovered. *VRT NWS* [online]. 2019 [cit. 2022-04-24]. Dostupné z: `https://www.vrt.be/vrtnws/en/2019/07/10/google-employees-are-eavesdropping-even-in-flemish-living-rooms/`.
7. KISKIS, Akvile. Android Microphone Eavesdropping. In: LATIFI, Shahram (ed.). *17th International Conference on Information Technology–New Generations (ITNG 2020)*. Cham: Springer International Publishing, 2020, s. 39–43. ISBN 978-3-030-43020-7.
8. WU, Longfei; DU, Xiaojiang; ZHANG, Hongli. An effective access control scheme for preventing permission leak in Android. In: *2015 International Conference on Computing, Networking and Communications (ICNC)*. 2015, s. 57–61. Dostupné z DOI: `10.1109/ICCNC.2015.7069315`.
9. ULLAH, Salim; KHAN, Muhammad Sohail; LEE, Choonhwa; HANIF, Muhammad. Understanding Users' Behavior towards Applications Privacy Policies. *Electronics*. 2022, roč. 11, č. 2. ISSN 2079-9292. Dostupné také z: `https://www.mdpi.com/2079-9292/11/2/246`.

10. SILVA, Pablo; AMORIM, Vicente J.P.; RIBEIRO, Filipe N.; MUZETTI, Igor. PrivacyMod: Controlling and Monitoring Abuse of Privacy-Related Data by Android Applications. In: *2015 Brazilian Symposium on Computing Systems Engineering (SBESC)*. 2015, s. 42–47. Dostupné z DOI: 10.1109/SBESC.2015.15.
11. ZHAO, Leah; WONG HON CHAN, Neil; YANG, Shanchieh Jay; MELTON, Roy W. Privacy Sensitive Resource Access Monitoring for Android Systems. In: *2015 24th International Conference on Computer Communication and Networks (ICCCN)*. 2015, s. 1–6. Dostupné z DOI: 10.1109/ICCCN.2015.7288451.
12. *The history of Android: The evolution of the biggest mobile OS in the world* [online]. 2021 [cit. 2022-04-23]. Dostupné z: https://www.androidauthority.com/history-android-os-name-789433/.
13. *Platform Architecture* [online]. 2021 [cit. 2022-04-23]. Dostupné z: https://developer.android.com/guide/platform.
14. SADOWSKA, Paulina. Android Runtime — How Dalvik and ART work? *ProAndroidDev* [online]. 2021 [cit. 2022-04-23]. Dostupné z: https://proandroiddev.com/android-runtime-how-dalvik-and-art-work-6e57cf1c50e5.
15. *Android Debug Bridge (adb)* [online]. 2022 [cit. 2022-04-23]. Dostupné z: https://developer.android.com/studio/command-line/adb.
16. *dumpsys* [online]. 2020 [cit. 2022-04-23]. Dostupné z: https://developer.android.com/studio/command-line/dumpsys.
17. *Streamlit documentation* [online]. © 2022 [cit. 2022-04-23]. Dostupné z: https://docs.streamlit.io/.
18. LUCENTE, Paolo. *DOCUMENTATION* [online]. 2021 [cit. 2022-05-07]. Dostupné z: https://github.com/pmacct/pmacct/blob/master/FAQS.
19. *What is 1e100.net? - Google Help* [online]. © 2022 [cit. 2022-05-04]. Dostupné z: https://support.google.com/faqs/answer/174717.
20. DETERS, John. *How to get rid of ad.doubleclick.net malware?* [Online]. 20207 [cit. 2022-05-06]. Dostupné z: https://security.stackexchange.com/a/226014.
21. *About the AdSense code - Google AdSense Help* [online]. © 2022 [cit. 2022-05-07]. Dostupné z: https://support.google.com/adsense/answer/9274634?hl=en.
22. SAD-EXCITEMENT9311. *r/ControlD - Comment by u/Sad-Excitement9311 on "Blocking request userlocation.googleapis.com"*. 2021. Dostupné také z: https://www.reddit.com/r/ControlD/comments/ok64q7/comment/h57xp0n/?utm_source=share&utm_medium=web2x&context=3.
23. 8206020236730627556, User. *Time Line Not Updating - Google Maps Community* [online]. 2022 [cit. 2022-05-04]. Dostupné z: https://support.google.com/maps/thread/143630682?hl=en&msgid=144007924.
24. *WHOIS 31.30.69.152 | Vodafone Czech Republic a.s. | AbuseIPDB* [online]. © 2022 [cit. 2022-05-05]. Dostupné z: https://www.abuseipdb.com/whois/31.30.69.152.
25. *WHOIS 85.205.100.141 | Vodafone Group Services GmbH | AbuseIPDB* [online]. © 2022 [cit. 2022-05-05]. Dostupné z: https://www.abuseipdb.com/whois/85.205.100.141.
26. SEKHAR, Komal; SEKHAR, Raja. *All you need to know about GPS/GNSS Integration on Android* [online]. 2019 [cit. 2022-05-05]. Dostupné z: https://www.pathpartnertech.com/all-you-need-to-know-about-gps-gnss-integration-on-android/.
27. *Sensors* [online]. 2020 [cit. 2022-05-06]. Dostupné z: https://source.android.com/devices/sensors?hl=en.

28. *Wi-Fi* [online]. 2022 [cit. 2022-05-05]. Dostupné z: https://source.android.com/devices/architecture/modular-system/wifi?hl=en.

29. SL, Uptodown Technologies. *Google Assistant Go (Android)* [online]. 2022 [cit. 2022-05-05]. Dostupné z: https://google-assistant-go.en.uptodown.com/android.

30. APPSAPK. *Navigation for Google Maps Go 10.30.2* [online]. © 2020 [cit. 2022-05-05]. Dostupné z: https://www.appsapk.com/navigation-for-google-maps-go-10-30-2/.

31. SL, Uptodown Technologies. *Google Text-to-Speech (Android)* [online]. 2022 [cit. 2022-05-05]. Dostupné z: https://google-text-to-speech.en.uptodown.com/android.

32. *Overview* [online]. 2022 [cit. 2022-05-07]. Dostupné z: https://source.android.com/devices/tech/connect/wifi-overview.

33. FOGFON. *xtra-daemon* [online]. 2019 [cit. 2022-05-05]. Dostupné z: https://github.com/fogfon/xtra-daemon.

# Obsah přiloženého média

- `README.md` ..... stručný popis obsahu média
- `app` ..... adresář se zdrojovými kódy mj. aplikace
- `data` ..... adresář s veškerými daty všech měření
- `info` ..... adresář sdružující informační soubory
- `monitoring` ..... skripty a nástroje využité při sběru dat
- `text` ..... zdrojové soubory textu