Scientific and Practical Cyber Security Journal (SPCSJ) 6(2): 48-60 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

მოწყობილობის მდებარეობასთან დაკავშირებული საფრთხეების შეფასება 5G ქსელის მაგალითზე

ASSESSMENT OF LOCATION BASED THREATS FOR DEVICES- A CASE STUDY OF 5G NETWORK

გიორგი ახალაია, კავკასიის უნივერსიტეტი. პ. სააკაძის ქუჩა, თბილისი, საქართველო მაქსიმ იავიჩი კავკასიის უნივერსიტეტი. პ. სააკაძის ქუჩა, თბილისი, საქართველო სერგი გნატიუკი, ეროვნული საავიაციო უნივერსიტეტი, უკრაინა, კიევი

Giorgi Akhalaia , Caucasus University , P.saakadze st1. Tbilisi, Georgia

Maksim Iavich, Caucasus University , P.saakadze st1. Tbilisi, Georgia

Sergiy Gnatyuk , National Aviation University, Kyiv, Ukraine

აბსტრაქტი:ბოლო წლებია 5G ტექნოლოგია საკომუნიკაციო სფეროს ერთ-ერთი უმნიშვნელოვანესი განხილვის თემა გახდა, განსაკუთრებით კიბერ უსაფრთხოებაში მომუშავე საზოგადოებისთვის. 3 ძირითადი კონცეპტით (გაუმჯობესებული მობილური ბროუდბენდი; ულტრა-საიმედო და დაბალი დაყოვნება; მანქანების მასიური რაოდენობით მიერთება), 5G ტექნოლოგია ცდება მობილური ქსელის ეკოსისტემას და ამით იწყება ახალი ეპოქა უკაბელო კომუნიკაციებში. ბუნებრივია, რომ ახალი ტექნოლოგიები, ფუნქციონალი წარმოქმნის ახალ საფრთხეებს - დაწყებული პროგრამული უზრუნველყოფიდან, დიზაინისა და იმპლემენტაციის პროცესის ჩათვლით. გამომდინარე იქიდან, რომ ვირტუალიზაცია იქნება 5G ქსელის ერთ-ერთი ძირითადი ელემენტი, მეხუთე თაობის ქსელი იქნება უფრო მეტად მოწყვლადი პროგრამულ უზრუნველყოფის საფრთხეების მიმართ. გაუმჯობესებული უსაფრთხოების მიუხედავად, 5G ქსელში მაინც რჩება დაუცველი ნაწილები, საიდანაც თავდამსხმელს შეუძლია გარკვეული მანიპულაციების ჩატარება. MITM (Man In The Middle - კაცი შუაში) ტიპის შეტევის გამოყენებით შესაძლებელი ხდება მომხმარებლის მოწყობილობის მოსმენა და სხვადასხვა მახასიათებლების, პარამეტრების შეცვლა. კვლევის მიზანი იყო დაგვედგინა რამდენად მარტივია MITM ის განხორციელება და გვეპოვა გადაწყვეტილება, უსაფრთხო დიზაინი, რომელიც შეამცირებდა MITM_ის რისკს. ასევე შეგვეფასებინა MITM ისგან გამოწვეული მოწყობილობის მდებარეობასთან დაკავშირებით არსებული საფრთხეები და კვლევის მაგალითზე დაგვედგინა, რომელი საფრთხეა შედარებით უფრო მაღალი რისკის შემცველი. კვლევის ფარგლებში, ვიპოვეთ კონცეპტუალური გადაწყვეტილება, რომლითაც შემცირდება რისკები. კვლევის მეორე ნაწილი ორიენტირებულია მდებარეობასთან დაკავშირებული საფრთხეების ექსპერიმენტულ შეფასებაზე.

საკვანძო სიტყვები: *5G ქსელის უსაფრთხოება, უსაფრთხო კომუნიკაცია, ლოკაციასთან დაკავშირებული საფრთხეები*

ABSTRACT: Over the last years, 5G technology has become one of the most significant topic for people working in network security industries. With the 3 key concept (enhanced mobile broadband; Ultra-reliable and low-latency communications and Massive machine type communications), 5G network will overcome the limitations of telecom and will arise ა new era of wireless communications. Upcoming functionalities, protocols, standards and services, as always, arise new vulnerabilities: starting from software, design, architecture and implementation processes too. Being virtualization a core component of 5G network, makes it more vulnerable to software-based attacks. Despite of some improved security mechanisms, there are left some weaknesses, that gives ability attackers to conduct various cyber attacks. Using MITM (Man In The Middle), attacker is able stand and sniff the traffic shared between user equipment and cell-towers. The goal of our research was to assess chances of making MITM in 5G network and find the solution, new design to minimize the risk. The second main goal was to determine location based threats in terms of user equipment, raised after MITM and analyze which of them is more dangerous and has the highest probability of

happening. In the framework of research, we have found conceptual solutions, that will lower the risk of MITM and it results. The second part of our study is oriented on experimental work.

KEYWORDS: *5G Network Security, Secure Communications; Location-Based Threats*

1. შესავალი

ტექნოლოგიურად განვითარებულმა და ძლიერი ეკონომიკის მქონე ქვეყნებმა უკვე დაიწყეს მეხუთე თაობის ქსელის დანერგვა. 2021 წლის 14 იანვარს, 5G ქსელის უსაფრთხოებასთან დაკავშირებით ამერიკის შეერთებულ შტატებსა და საქართველოს შორის გაფორმდა ურთიერთგაგების მემორანდუმი. რომლის თანახმად ქვეყნებს მჭიდრო კომუნიკაცია ექნებათ და ამერიკის შეერთებული შტატები დაეხმარება საქართველოს მეხუთე თაობის ქსელის დანერგვასა და მისი უსაფრთხოების უზრუნველყოფაში.

განვითარება, მითუმეტეს ტექნოლოგიური ევოლუცია არასდროსაა წრფივი. მისი მიმართულება და პროგრესის ხარისხი დამოკიდებულია ახალ საჭიროებაზე, გადაუდებელ აუცილებლობაზე. ხელოვნური ინტელექტის განვითარებამ კიდევ უფრო დააჩქარა ავტომატიზაციის, თვითმართვადი და სხვადასხვა ტიპის დისტანციური სერვისების განვითარება. შესაბამისად, უკვე გამოიკვეთა პრობლემა, როცა ინფორმაციის სწრაფი გადაცემა(მინიმალური დაყოვნება - Extremely Low Latency) იყო შემაფერხებელი, მაგალითად დისტანციური პროცესების რეალურ დროში სინქრონიზაციისათვის, ასევე მნიშვნელოვნად გაიზარდა ქსელზე მიერთებული მოწყობილობების (მაგ: IoT) რაოდენობა მჭიდრო პერიმეტრზე, რაც არსებული სისტემებისთვის პრობლემას წარმოადგენდა. შესაბამისად დაიწყეს მეხუთე თაობის ქსელზე მუშაობა. 5G (5^{th} Generation) ქსელი არის არამარტო მობილური ინტერნეტის განვითარების ერთ-ერთი საფეხური არამედ უკაბელო ქსელის ახალი ეპოქის დასაწყისი. ხელოვნური ინტელექტის გამოყენებითა და 5G ქსელის საშუალებით სინქრონში იქნება შესაძლებელი მონაცემთა ანალიზი და გადაწყვეტილებების სწრაფი მიღება, გადაცემა და სინქრონიზაცია სხვადასხვა სისტემას შორის.

მეხუთე თაობის ქსელი თავისი უპირატესობიდან გამომდინარე მნიშვნელოვნად განავითარებს/შექმნის ახალ IoT ეკოსისტემას, ავტოპილოტიანი ავტომობილების ინდუსტრიას, ჯანდაცვის სისტემის სერვისებს (მაგ: დისტანციური ოპერაციები); დრონებისა და სხვადასხვა ჭკვიანი მოწყობილობების ფუნქციონალის გაზრდა/ავტომატიზაციას. ხელს შეუწყობს ისეთი სერვისების შექმნას, რომლისთვისაც კრიტიკულად მნიშვნელოვანია ინფორმაციის სწრაფად, მინიმალური დაყოვნებით გადაცემა და/ან სხვა სისტემასთან სტაბილური და სწრაფი კომუნიკაცია.

5G ქსელის განვითარებაზე მუშაობს 3GPP (3rd Generation Partnership Project). რომელიც წარმოადგენს სხვადასხვა ორგანიზაციის კონსორციუმს. პერიოდულად ხდება წევრი ორგანიზაციების შეკრება და სამოქმედო გეგმის დასახვა. ITU_მ მეხუთე თაობის ქსელის KPI_დ დაასახელა:

- > 10Gb/s - არანაკლებ 10 გიგაბიტ/წამი პიკური სიჩქარე (eMBB)

- > 1M/km^2 - არანაკლებ 1 მილიონი მოწყობილობის დაკავშირების შესაძლებლობა კვადრატულ კილომეტრზე. (mMTC). ასეთი სიმჭიდროვე აღებულია IoT მოწყობილობებიდან გამომდინარე.
- < 1ms Latency - არაუმეტეს 1 მილიწამი დაყოვნება.(URLLC) [1]

რაც შეეხება 5G_ის სამუშაო სპექტრს, შემდეგნაირად არის დაგეგმილი:

1. Low-band -- < 1 GHz
2. Mid-band -- 1 GHz – 6 GHz
3. High-band(mmWave) – 6 GHz – 100 GHz

Low-Band - მოიცავს 1GHz მდე სპექტრს. მისი უპირატესობაა მჭიდროდ დასახლებული რეგიონის დაფარვა. ნაკლებ პრობლემა უქმნის შენობა/ნაგებობები. მაგრამ Peak Data Speed დაახლოებით 100 Mbps_ია.

Mid-Band - იგულისხმება 1GHz დან 6GHz მდე სპექტრს. Low-band ისგან განსხვავებით უფრო მეტი გამტარუნარიანობა და ნაკლები დაყოვნება აქვს. თუმცა შედარებით მეტ დაბრკოლებას უქმნის ნაგებობები ვიდრე Low-band_ს. პიკური სიჩქარე დაახლოებით 1 Gbps_ია.

High-Band - ძირითადად ამ სპექტრს მოიაზრებენ როცა 5G ქსელზეა საუბარი. ამ სპექტრის საშუალებით შესაძლებელი ხდება მინიმალური დაყოვნებით, პიკური სიჩქარის ათობით Gbps_მდე გაზრდა. ხშირად მოიხსენიებენ როგორც mmWave ტექნოლოგიად. ზემოთ ჩამოთვლილი სპექტრული დანაყოფებიდან, სწორედ High-band წარმოადგენს მთავარ რგოლს 5G ქსელის იმპლემენტაციაში.[2]

5G ქსელის ერთ-ერთი მთავარი სამიზნე კატეგორია IoT მოწყობილობებია. მნიშნელოვანი პროგრესი უნდა იყოს ქსელის ისე მუშაობა, რომ IoT მოწყობილობების ენერგო მოხმარება მინიმუმამდე დავიდეს(რა თქმა უნდა ქსელის კუთხით). თუმცა 5G ტექნოლოგიის მომხმარებლისთვის ერთ-ერთი ყველაზე შემჩნევადი პრობლემა მოწყობილობის ელემენტის სწრაფი დაცლა, ე.წ. Battery Drain_ია. CNET ის ტესტერებმა ჩაატარეს ცდა: აიღეს 5G მხარდაჭერის მქონე ორი მობილური, რომლებიც ჯერ ამუშავეს მე_5 თაობის ქსელზე და შემდეგ მის გარეშე. პირველ შემთხვევაში MOTO Z3 ის ელემენტი 5G ქსელზე გადაბმულად მუშაობის შედეგად 4 საათში ბოლომდე დაიცალა. რაც შეეხება მეორე ტესტს, გამოიყენეს Galaxy S10. ამ შემთხვევაში, 5G ზე მუშაობის შედეგად 4 საათში ელემენტის დამუხტვის პროცენტი განახევრდა, მაშინ როცა გადაბმულად ტელეფონი დამუხტვის გარეშე 18 საათი მაინც უნდა მუშაობდეს.[3]

აღნიშნული პრობლემის შესახებ წერს Samsung_იც. მიზეზად კი, სხვა ექპერტების მსგავსად, გადამრთველს ე.წ. switch_ს ასახელებს. 5G ქსელი ამ ეტაპზე გამოიყენება მხოლოდ მონაცემთა გადაცემისთვის, უფრო სამომხმარებლო ენაზე რომ ვთქვათ, ინტერნეტისთვის.[4] აქედან გამომდინარე, მობილურ ტელეფონს პარალელურ რეჟიმში უწევს 4G ან 3G/2G ქსელთან კავშირი, რათა შეუფერხებლად მიიღოს და/ან განახორციელოს სატელეფონო ზარი, მოკლე ტექსტური შეტყობინება - SMS. სტატიაში ნათქვამია ისიც, რომ ელემენტის სწრაფი დაცლის გარდა, ამან შეიძლება მოწყობილობის შესამჩნევად გაცხელება გამოიწვიოს. ასევე მნიშნელოვანი ფაქტორია ქსელის მუდმივი გადართვა 5G დან 4G/3G ზე. გამომდინარე იქიდან, რომ ალგორითმის მიხედვით ტელეფონი მუდმივად ცდილობს სტაბილური ინტერნეტ სიჩქარის შენარჩუნებას, ხოლო 5G ქსელის დაფარვა არ არის კარგი და მნიშვნელოვნად დამოკიდებულია ანძინად დაშორებულ მანძილზე, დახრის კუთხეზე(ანძასა და მიმღებ მოწყობილობას შორის) მობილური ტელეფონი ინტერნეტ სერვისის გადაცემას მუდმივად რთავს 5G დან 4G/3G ზე. აქედან გამომდინარე ხშირი

გადართვა/გადმორთვა მოიხმარს დამატებით ენერგიას, რაც საბოლოო ჯამში ელემენტის სწრაფ დაცლაში აისახება. ექსპერტების აზრით ტექნოლოგია ჯერ კიდევ დახვეწის პროცესშია და დროთა განმავლობაში გაუმჯობესდება გადართვის (Switch) მექანიზმი. თუმცა, არ უნდა დაგვავიწყდეს, რომ ერთ-ერთი მთავარი პრობლემა, საფრთხე MITM შეტევაა, რომელიც გარდა ინფორმაციის გაჟონვისა, შემდეგ სხვადასხვა ტიპის შეტევის საშუალებასაც იძლევა.

2. 5G_ს უსაფრთხოება

მეხუთე თაობის ქსელის უსაფრთხოება კიდე უფრო კომპლექსურია მისი არქიტექტურიდან გამომდინარე. მონაცემთა ცენტრების, cloud ტექნოლოგიებისა და თითოეული endpoint ის დაცვა კრიტიკული გახდა რადგან ქსელის დანერგვის ერთ-ერთი core კომპონენტია ვირტუალიზაცია და ქსელის ფუნქციათა ვირტუალიზაციის ინფრასტრუქტურა. გამომდინარე იქიდან, რომ 5G ქსელში ჩაირთვება სხვადასხვა კატეგორიის, მწარმოებლის, შესაბამისად firmware ისა და აპარატურული არქიტექტურის მქონე სისტემა/მოწყობილობა, რომლებიც განსხვავებულ ტექნოლოგიებს იყენებენ მათი ცალ-ცალკე არსებული სისუსტე, გადმოყვება სისტემაში და უკვე გახდება სისტემის შემადგენელი სისუსტე. ასევე ყურადსაღებია LBS(Location Based Service) ტიპის სერვისები, მომხმარებლის პერსონალური ინფორმაციაზე, მოწყობილობის სხვადასხვა სერვისის გამოყენებისას გაცემული პირადი ინფორმაცია საბოლოოდ დასაცავი აღმოჩნდება. 5G ქსელის შემთხვევაში ჩნდებიან ახალი აქტორებიც, მაგალითად - ვირტუალური მობილური ოპერატორები, კომუნიკაციების სერვის პროვაიდერები და ქსელის ინფრასტრუქტურის პროვაიდერები, რომლებთაც თავიანთ განსხვავებული უსაფრთხოების პოლისები აქვთ. შესაბამისად მათი საერთო სისტემაში მოყვანა იქნება აუცილებელი. ის ფაქტი, რომ 5G ქსელი წინა თაობებთან შედარებით უფრო მეტად software based და cloud-based ია, უკეთესი მონიტორინგის სისტემის იმპლემენტაციის საშუალებას იძლევა. ქსელის სეგმენტირება (Network Slicing) ის საშუალებით კი შესაძლებელია კატეგორიებად დაიყოს და თითოეულ მათგანზე მორგებული დაცვის მექანიზმები გაიმართოს.

მართალია 4G_სგან განსხვავებით 5G ქსელი მომხმარებლის უსაფრთხოება შედარებით დახვეწილია, მაგრამ მაინც რჩება ინფორმაციის ნაწილი, რომელიც ე.წ. clear text_ად მიმოიცვლება ქსელში ბაზასთან დაკავშრებისას. რომელიც შემდეგ სხვა ინფორმაციის მოპარვისთვის შეიძლება გამოიყენოს თავდამსხმელმა. ეს აჩენს ე.წ. Fake Base Station Attack ის საფრთხეს. ამ დროს მესამე პირი მომხმარებელს თავს აჩვენებს თითქოს ის არის რეალური cell tower, რის შედეგადაც მასთან დაკავშირებას ცდილობს მსხვერპლი. საბოლოოდ კი თავდამსხმელი შეძლებს ტრაფიკის მოსმენას და მასზე სხვადასხვა მანიპულაციას. მსგავს იმიტირებულ შეტევაზე Black Hat 2019 ის “New Vulnerabilities in 5G Networks” სესიაზე ისაუბრა Altaf Shaik. მათმა ჯგუფმა შექმნა fake base station და აკვირდებოდნენ მოწყობილობებიდან გაგზავნილ ინფორმაციას, რომელთა ნაწილი დაუშიფრავია. დაკვირვება ხდებოდა შემდეგ კატეგორიებად: მწარმოებელი, მოდელი, ოპერაციული სისტემა, ვერსია და რისთვის გამოიყენება(use case).[5] ამის შედეგად მათ ქონდათ უკვე სრული სურათი, რუკა თუ საიდან რა მოწყობილობა რა ფუნქციით დატვირთული უკავშირდებოდა ქსელს. ეს არის **MNmap (Mobile Nmap)**. შედეგად თავდამსხმელს აქვს ქსელზე მიერთებული მოწყობილობების სრული სურათი და შესაბამისად შეძლებს კონკრეტული სამიზნე კატეგორიისთვის დაგეგმოს სხვა, უფრო მაღალტექნოლოგიური შეტევა.

მანამდე სანამ Device_დან base თან გაგზავნილი ინფორმაცია ჯერ კიდევ clear text ია, ანუ დაუშიფრავია შესაძლებელია მისი hijack(გატაცება) და მისი სურვილისამებრ შეცვლა. მაგალითად კავშირის შენელება, device ის იდენტიფიკაციის შეცვლა, MIMO ფუნქციონალის ჩამოშორება, battery drain და სხვა. **MITM**_ით PSM პარამეტრის თავის არიდებაა შესაძლებელი. რომლის შედეგადაც მოწყობილობა მუდმივად სკანირების რეჟიმშია და ეძებს დასაკავშირებელ hosts. შედეგად კი ელემენტი დაახლოებით 5 ჯერ უფრო სწრაფად დაჯდება. წყაროებში ეს შეტევა მოხსენებულია როგორც **Battery Drain.**

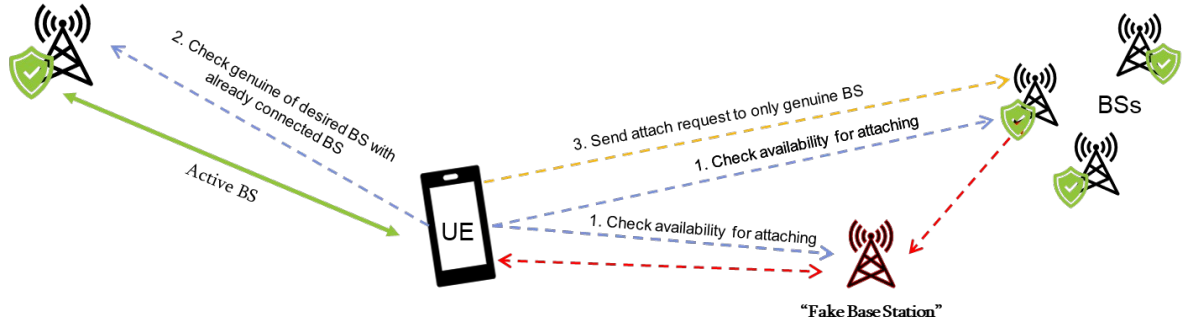
მკვლევარების საუბრობენ ასევე 5G Downgrade შეტევაზე(ზოგ წყაროში Bidding Down Attack წერია). ამ დროს სამიზნე მოწყობილობის კავშირის ჩამოქვეითება (Downgrade) ხდება 3G ან 4G ქსელზე. შემდეგ კი ამ ტექნოლოგიებზე არსებულ სისუსტეებზე უპირატესობის მოპოვება ხორციელდება.

ასევე მნიშნელოვანია ამ ტექნოლოგიების სწორი იმპლემენტაცია. რაც არ უნდა კარგად გამართონ 5G_ზე მომუშავე ორგანიზაციებმა უსაფრთხოების პროტოკოლები და სტანდარტები, თუ სერვის პროვაიდერმა/ოპერატორმა სტანდარტის დანერგვისას არასწორად შეასრულა პირობები ან არასრულად(მისი ხარჯიდან გამომდინარე) მაშინ სისტემის უსაფრთხოება ისევ რისკ ქვეშ დგება. მსგავსი ქეისები კი საკმაოდ იყო 4G ტექნოლოგიების გაშვებისას, როცა ოპერატორებმა ხარჯის შემცირების მიზნით გარკვეული პროცედურები არ შეასრულეს. მსგავსი პრობლემა დგება 5G_ს შემთხვევაშიც. თუმცა მსგავსი ტიპის პროცესი შეიძლება სახელმწიფომ დაარეგულიროს სხვადასხვა საკანონმდებლო მექანიზმით. მაგალითად USA ში, FCC (კომუნიკაციების ფედერალური კომისია) გააკონტროლებს სტანდარტის დანერგვას.

ყველა ტექნოლოგიას, სერვისს თუ ფუნქციონალს აქვს უსაფრთხოების გარკვეული პრობლემა. 5G ქსელს, კერძოდ ვირტუალიზაციის ნაწილში აქვს უსაფრთხოების საკმაოდ მნიშვნელოვანი პრობლემები. ქსელის პროცესების სამართავად გამოიყენება AI. ქსელის მასშტაბურობიდან გამომდინარე, AI Operator Hijack შეტევისას შედეგები იქნება გაცილებით მასშტაბური, ვიდრე ჩვეულებრივ შემთხვევაში. თუ ვირტუალიზაციის პლათფორმაზე განახორციელებენ შეტევას, რომელიც core მექანიზმია ქსელის, მთავარი სამართავი პანელი მაშინ წარმოიდგინეთ რა დაემართება სხვადასხვა IoT მოწყობილობას, მაგალითად ინპლანტებს, უპილოტო მანქანებს, რა მოხდება დისტანციური ოპერაციებისას.

3. უსაფრთხო დიზაინის კონცეპტი

არსებული დიზაინი, თეორიული კვლევისა და პრაქტიკული ექსპერიმენტების თანახმად მოწყვლადია MITM ტიპის შეტევების მიმართ. რომელიც მიიჩნევა ერთ-ერთ ყველაზე მძლავრ, ეფექტურ ქსელურ შეტევად. ჩვენი კვლევის შედეგად მიღებული ახალი, უსაფრთხო დიზაინის კონცეპტი, მნიშვნელოვნად ამცირებს ქსელში ე.წ. ცრუ ანძების ეფექტურობას.



ილუსტრაცია 1

ილუსტრაცია 1_ზე მოცემულია კონცეპტუალური დიზაინის მიხედვით როგორ მოხდება ქსელში მოწყობილობის ჩართვა, ოპერატორის ანძასთან დაკავშირება. მწვანე სიმბოლოთი აღნიშნულია ავტორიზებული ანძები, ხოლო წითლად მოცემული ცრუ ანძა, რომელიც ასრულებს MITM ტიპის შეტევას. ჩვენი იდეის მიხედვით, ანძებს უნდა ქონდეს წინასწარ განსაზღვრული ალგორითმი, სია, რომლითაც შეძლებენ ერთმანეთის ავთენტურობის გადამოწმებას, ამ შემთხვევაში სერვისს შეასრულებენ მომხმარებლის მოწყობილობისთვის. განხილულია შემთხვევა, როდესაც მოწყობილობას უკვე აქვს აქტიური კავშირი ლეგიტიმურ ანძასთან. ქსელის მუშაობის პრინციპიდან გამომდინარე, მუდმივად ეძებს უფრო ძლიერი სიგნალის მქონე ანძას. შესაბამისად როდესაც იპოვის ცდილობს ახალ ანძაზე გადართვას. ჩვენი დიზაინის მიხედვით, სამიზნე ანძასთან დაკავშირების მოთხოვნის გაგზავნამდე ითხოვს მაიდენტიფიცირებელ ინფორმაციას, რომელსაც ამოწმებს უკვე აქტიურ ანძასთან - რამდენად ავტორიზებულია სამიზნე ანძა ქსელში. თუ, აქტიური ანძა დაუდასტურებს სამიზნე ანძის ავთენტურობას, მაშინ მოწყობილობა დაიწყებს ახალ ანძაზე გადართვის პროცედურებს.

ამ დიზაინის ერთ-ერთი მნიშვნელოვანი შეზღუდვაა ის შემთხვევა, როდესაც არ გვაქვს აქტიური კომუნიკაცია რეალურ ანძასთან ან გვაქვს მაგრამ არასტაბილური სიგნალია. პირველი შეიძლება მოხდეს მაშინ, როდესაც ე.წ. ფრენის რეჟიმიდან გადავდივართ ჩვეულებრივ რეჟიმზე და ვიწყებთ ქსელში ჩართვას, ან მაგალითად როდესაც მობილურ მოწყობილობას ხელახლა ვრთავთ. არასტაბილური სიგნალი კი შიდა როუმინგის დროს შეიძლება მოხდეს. მაგალითად, როდესაც კარგი დაფარვა არ აქვს ოპერატორს. შესაბამისად ამ დროს ვერ მოხდება გადამოწმება სამიზნე ანძის ავთენტურობის. ამ შემთხვევაში შეიძლება იყოს წინასწარ, მოწყობილობაში ინტეგრირებული სია, დაახლოებით სერთიფიკატის მსგავსი, რომლითაც თავისივე თავთან გადაამოწმებს სამიზნე ანძის რეალურობას.

ეს დიზაინი თავის მხრივ კიბერ საფრთხეების რისკს გაზრდის მობილური ოპერატორების ანძების მიმართს. ეს ბუნებრივიცაა, რადგან ყოველი ახალი დაცვის მექანიზმი ამისამართებს შეტევის ვექტორებს, სხვა შედარებით სუსტი წერილის მიმართ. ასევე ნაკლებად ეფექტური შეიძლება იყოს საერთაშორისო როუმინგის დროს.

3.1.ექსპერიმენტული კვლევა

კვლევისას განვითარებული თეორიული იდეების განსახორციელებლად, ჩავატარეთ ექსპერიმენტი. მიკრო ლაბში, მიკრო კომპიუტერების - Raspberry Pi_ს გამოყენებით

განვახორციელეთ მოწყობილობის ქსელთან მიერთების სიმულაცია. პროცესის სამართავად გამოვიყენეთ კომპიუტერი, Kali OS ის ოპერაციული სისტემა და სხვადასხვა პროგრამული პაკეტი. Raspberry Pi_ს ნაწილი წარმოადგენდა მობილური ოპერატორის ანძის სიმულაციას, ხოლო ნაწილი მომხმარებლის მოწყობილობას. (ცხრილი 1) როდესაც მომხმარებლის მოწყობილობებს მივუთითეთ, რომ წინასწარ გადაემოწმებინა ბაზის ავთენტურობა, არცერთი შემთხვევა აღარ ყოფილა “fake base station” თან დაკავშირების. ფაქტობრივად, მოწყობილობები აღარ აგზავნიდნენ ცრუ ანძებთან დაკავშირების მოთხოვნას. ეს შეიძლება ჩაითვალოს როგორც ჩვენეული გადაწყვეტილების დადებით შედეგად და მოგვცეს პოზიტიური მოლოდინი ალგორითმის რეალურ შემთხვევაში მუშაობისთვის. მაგრამ, აქვე ყურადსაღებია ის ფაქტი, რომ რეალური სისტემა ბევრად დატვირთულია მოწყობილობებისა და ანძების რაოდენობის გათვალისწინებით, შესაბამისად აუცილებელია რეალურ სისტემაზეც ტესტირება. გამომდინარე იქიდან, რომ 5G ქსელი ამ შემთხვევაში არ გვაქ, ტესტირება მიმდინარეობა 4G ქსელის მაგალითზე. თუმცა, დაკავშრების პროცესი მსგავსია, ამიტომ ეს კვლევის შედეგებზე უარყოფით გავლენას არ მოახდენდა.

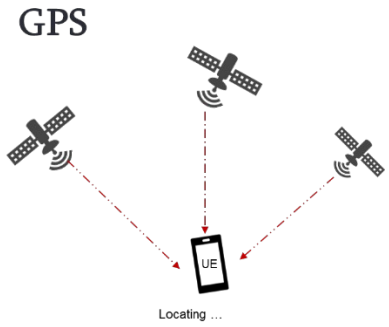
ექსპერიმენტის მეორე ნაწილში განვიხილეთ, ისეთი შემთხვევა როდესაც მოწყობილობა ე.წ. “Roaming”_შია. ანუ როდესაც აქტიური კავშირი ბაზასთან არ აქვს ან კავშირი არასტაბილურია. ამ შემთხვევაში წინასწარვე მივაწოდეთ სანდო ანძების სია. შედეგების მიხედვით, ორივე შემთხვევა შეიძლება გამოვიყენოთ ერთად, როგორც დამზღვევი სისტემა, რომელიც უზრუნველყოფს ქსელში მეტ უსაფრთხოებას. მეორე შემთხვევაში, პირველთან შედარებით პროცესი უფრო სწრაფად მიმდინარეობს, თუმცა მნიშნელოვანი კომპონენტი იქნება ახალი ანძების შესახებ ინფორმაციის მიწოდება მოწყობილობისთვის და/ან უკვე არსებული ინფორმაციის მთლიანობის/უცვლელობის დაცვა.

მოწყობილობა	**რაოდენობა**	**დანიშნულება**
Raspberry Pi (LTE მოდულით)	40	20 - ანძის სიმულატორი, 5 - ცრუ ანძის სიმულატორი 15 - მომხმარებლის მოწყობილობა
კომპიუტერი Kali OS_ით	2	პროცესის სამართავად, სიმულაციისთვის
შედეგები		
ალგორითმის ტიპი	**წარმატება/ ჩავარდნა**	**კომენტარი**
აქტიური ანძიდან აუთენთიფიკაცია	წარმატება	15/15
შიდა ცხრილიდან აუთენთიფიკაცია	წარმატება	15/15
საბოლოო შეფასება		
ალგორითმებმა იმუშავა, თუმცა გაიზარდა დაყოვნება		

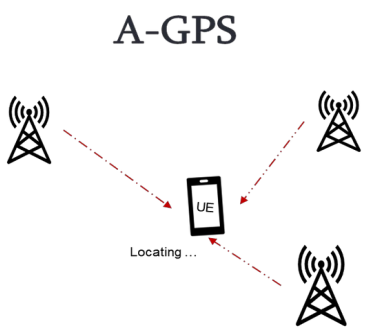
ცხრილი 1. ექსპერიმენტში გამოყენებული ინფრასტრუქტურა

4. ლოკაციასთან დაკავშირებული საფრთხეები

მოწყობილობის ადგილმდებარეობის დადგენის 2 ძირითადი მეთოდი არსებობს: GNSS ტექნოლოგიების გამოყენებით ან A-GPS მეთოდით. პირველი გულისხმობს GNSS სატელიტების გამოყენებით მოწყობილობის მდებარეობის განსაზღვრას, რაც არსებული მეთოდებიდან ყველაზე ზუსტია, ხოლო მეორე (A-GPS) მობილური ოპერატორის ანძების მიხედვით მომხმარებლის მოწყობილობის ადგილმდებარეობის გადათვლას/დაანგარიშებას. ორივე მეთოდს აქვს თავისი უპირატესობა და შეზღუდვები: GNSS ის შემთხვევაში, აუცილებელია მოწყობილობას პირდაპირი ხედვა ქონდეს სატელიტებთან, ანუ ე.წ. ღია ცის პრინციპი მუშაობს, მაგრამ ყველაზე მაღალი სიზუსტეს იძლევა (3-5 მ ცდომილება სამომხმარებლო მოწყობილობებში), ხოლო მეორე A-GPS, მობილური ოპერატორის მინიმუმ 3 ანძის საშუალებით ითვლის თავის მდებარეობას. ეს ნაკლებად ზუსტია, მაგრამ შეუძლია დახურულ სივრცეებშიც, მაგალითად შენობებშიც გადაითვალოს მოწყობილობის კოორდინატები. (ფიგურა 1, 2)



ფიგურა 1. GPS მეთოდი

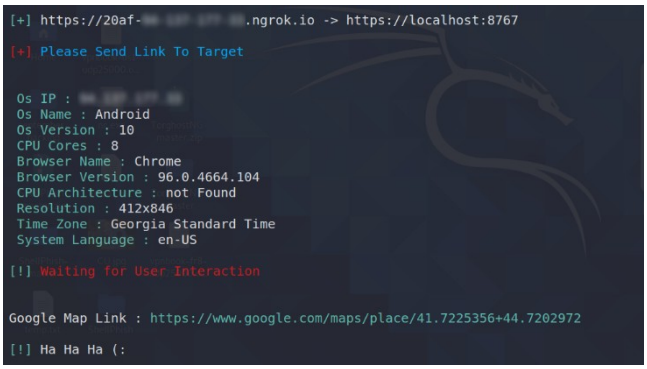


ფიგურა 2. A-GPS მეთოდი

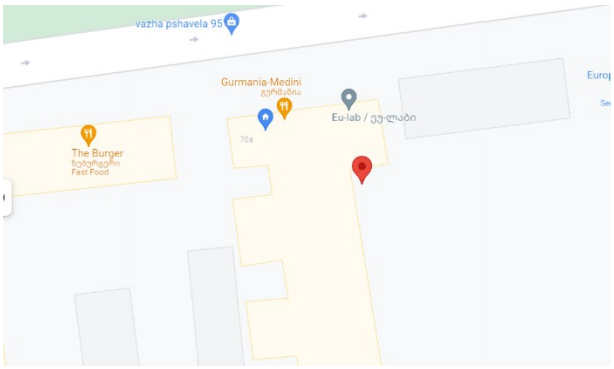
გამომდინარე იქიდან, რომ A-GPS ის შემთხვევაში მოწყობილობა იყენებს მობილური ოპერატორის ანძების დეტალებს, კოორდინატებს თავისი მდებარეობის დასაზუსტებლად, MITM ის შეტევის შემთხვევაში, როდესაც ე.წ. “Fake Base Station“_ის შეტევა ხორციელდება, დიდია საფრთხე, რომ მოწყობილობის ლოკაცია არასწორად გადაითვალოს, რადგან თუ მიწოდებული(გამოთვლისას გამოყენებული) ინფორმაცია არასწორი იქნება, მაშინ შედეგსაც არასწორს მივიღებთ. ეს კი დიდ პრობლემას შეუქმენის ე.წ. Location-Based სერვისებს, მათ შორის 911/112 სერვისებისთვის საჭირო პროცესებს. ასევე, გასათვალისწინებელია ის ფაქტიც, რომ GNSS ს მეთოდის შემთხვევაში აუცილებელია მობილურ მოწყობილობაში გააქტიურებული იყოს GPS მოდული, ხოლო A-GPS მეთოდი, ქსელის მუშაობის პრინციპიდან გამომდინარე მობილურ მოწყობილობაში ავტომატურად აქტიურია (გარდა ე.წ. ფრენის რეჟიმისა). ეს კი, შესაძლოა, რაღაც შემთხვევებში ამარტივებდეს LBS ზე შეტევას. კვლევისას სხვადასხვა სიმულაციური ექსპერიმენტი ჩავატარეთ, რომლის დეტალებიც შემდეგ თავშია აღწერილი.

4.1. ექსპერიმენტული კვლევა

კვლევისას ჩავატარეთ რამდენიმე ექსპერიმენტი, რათა დაგვედგინა რომელი მეთოდი, გზაა შედარებით მარტივი, რომლითაც საშუალება გვექნება დავადგინოთ მომხმარებლის მდებარეობა მათი „ნებართვის გარეშე“. (ცხრილი 2). პირველ შემთხვევაში გამოვიყენეთ მზა ხელსაწყო, Storm-braker (ფიგურა. 9, 10). [6]

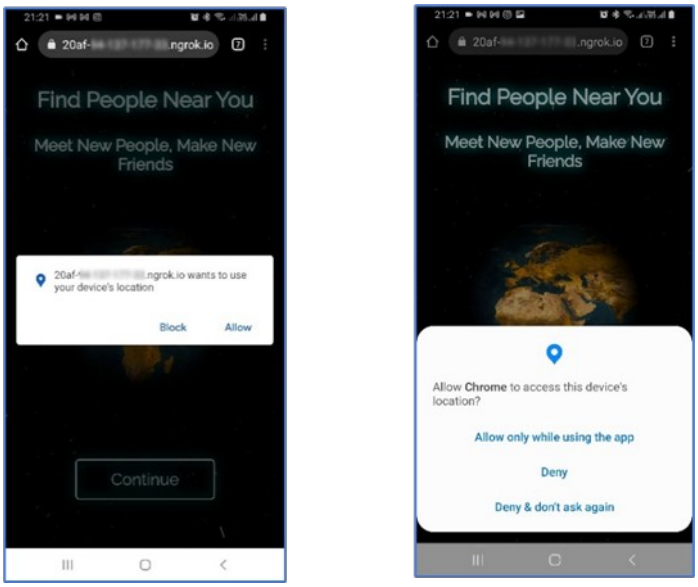


ფიგურა. 9



ფიგურა. 10

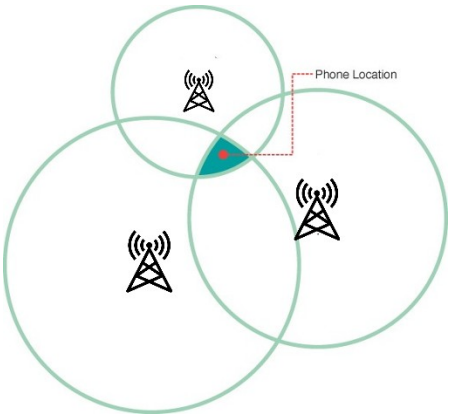
ის არის მზა პროგრამული უზრუნველყოფა, რომელიც საშუალებას გვაძლევს მომხმარებლის მოწყობილობიდან წამოვიღოთ GNSS კოორდინატები. თუმცა, კვლევამ აჩვენა, როგორც მოსალოდნელი იყო, რომ საკმაოდ „ხმაურიანია“. რადგან მომხმარებელი წინასწარ განსაზღვრულ ბმულზე გადასვლისას ღებულობს გამაფრთხილებელ შეტყობინებას, რომ აპლიკაცია/სერვისი ცდილობს მის ლოკაციაზე წვდომის მოპოვებას და ამისთვის ითხოვს ნებართვას. (ფიგურა 11)



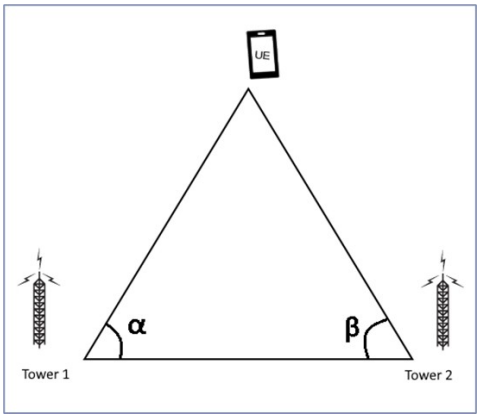
ფიგურა 11

გამომდინარე იქიდან, რომ მოწყობილობა მუდმივ რეჟიმში არ ითვლის თავის მდებარეობას GNSS ტექნოლოგიების გამოყენებით(საუბარია თანამგზავრებზე), აპლიკაციით ასეთი ინფორმაციის მოპარვისას, მომხმარებელი ღებულობს შეტყობინებას, რომ აპლიკაცია ცდილობს მოდულის გამოყენებას და მდებარეობის დადგენას. ამ მეთოდის უარყოფითი

მხარეა ისიც, რომ თუ GPS მოდული გამორთულია, ან მოწყობილობა დახურულ სივრცეშია (მაგალითად შენობაში) მაშინ ვერ იმუშავს. ამ შემთხვევაში უფრო ეფექტურია, მომხმარებლის მოწყობილობიდან თუ A-GPS ის მონაცემებს წამოვიღებთ. რადგან მობილური მოწყობილობის და ოპერატორების მუშაობის პრინციპიდან გამომდინარე, მოწყობილობა მუდმივად ამოწმებს დაფარვის არეალში მყოფ ანძებს, შესაძლებელია ამ ინფორმაციით, მონაცემებით და ტრიანგულაცია/ტრილატერაციის მეთოდით დადგინდეს მომხმარებლის მიახლოებითი მდებარეობა. არა ისეთივე ზუსტი როგორც GNSS ტექნოლოგიების შემთხვევაში, მაგრამ ასადევნებლად საკმარისი.

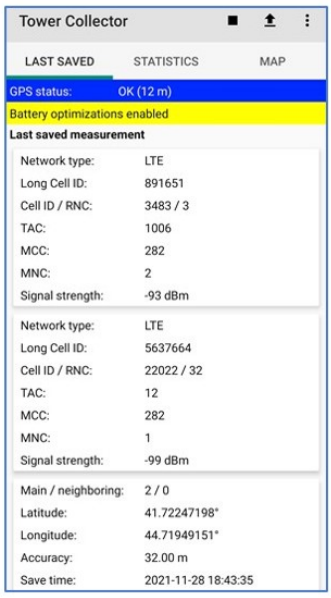


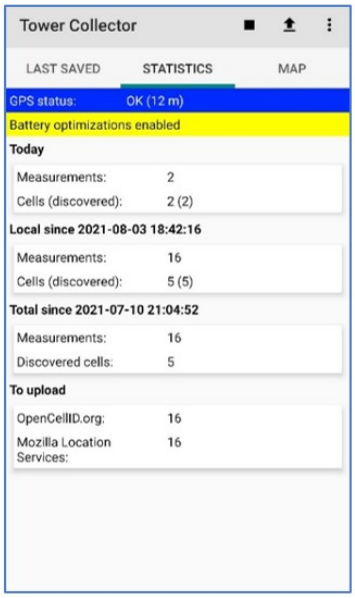
ფიგურა 12. ტრილატერაცია



ფიგურა 13. ტრიანგულაცია

არსებობს მზა ხელსაწყოები, რომელიც საშუალებას გვაძლევს ოპერატორის ანძების განლაგების რუკა შევქმნათ, რომელსაც შემდეგ მომხმარებლის მოწყობილობის მდებარეობის განსაზღვრისთვის გამოვიყენებთ. მაგალითად OpenCellID პროექტი. ჩვენ გამოვიყენეთ ანდროიდის მარკეტზე არსებული პროგრამა: “Tower Collector”. (ფიგურა 12, 13)





როგორც ფიგურაზე ჩანს, საკმაოდ დეტალურ ინფორმაციას ვიღებთ ანძების შესახებ, მათ შორის რაც მთავარია ID, კოორდინატები და სიგნალის სიძლიერე. აღსანიშნავია ფაქტი, რომ საკმაო მსჯელობის საგანია სიგნალის სიძლიერე, მკვლევართა ნაწილი თვლის, რომ ამ პარამეტრით შესაძლებელია ზუსტი მოწყობილობის ადგილმდებარეობის დადგენა. თუმცა, ფაქტია, რომ იმდენად კომპლექსური მახასიათებელია, რთულია ცალსახად რაიმეს თქმა. რადგან ძალიან ბევრი ფაქტორი ახდენს გავლენას სიგნალის სიძლიერეზე, მათ შორის რელიეფი და შენობები. რაც ყველაზე მნიშვნელოვანია, 5G ქსელის შემთხვევაში იმისათვის რომ მოწყობილობამ გამოიყენოს High-Band სპექტრი, ე.წ. mmWave, აუცილებელია რომ იყოს ძალიან ახლოს, პირდაპირი ხედვით ანძასთან. რადგან ამ სიხშირეების ტალღებს ყველაზე (წინა 2 თან შედარებით) მეტად ამახინჯებს შენობები. შესაბამისად, ეს შეიძლება გახდეს იმის მიზეზი, რომ 1 ანძითაც დადგინდეს მოწყობილობის მდებარეობა. რაც დიდ პრობლემას წარმოადგენს მომხმარებლის უსაფრთხოებისთვის.

კვლევისას გამოყენებული ინფრასტრუქტურა:

მოწყობილობა	**რაოდენობა**	**დანიშნულება**
Raspberry Pi (LTE და GPS მოდულებით)	30	10 - საბაზისო სადგური, 15 - ცრუ საბაზისო სადგური 5 - მომხმარებელი
GPS მოდულიანი მობილური მოწყობილობები	5	მომხმარებელი
Laptop (Kali OS)	2	ექსპერიმენტის მონიტორინგი და მართვა
შედეგები		
ალგორითმის ტიპი	**წარმ/ ჩავარნა**	**კომენტარი**
GPS (GNSS კოორდინატების მოწყობილობიდან აღება)	წარმატებული	Success with noise if GPS module was enabled. User interaction was needed. As they were alerted by the system
A-GPS (ინფორმაციის მოწყობილობიდან წამოღება)	წარმატებული	10/10
MITM by Fake BS	წარმატებული	10/10
ანძების ინფორმაციის(სიხშირეების, აქტიური ანძების) წამოღება	წარმატებული	8/10

ცხრილი 2

კვლევისას დადგინდა, რომ A-GPS ის მონაცემების წამოღება ნაკლებად ხმაურიანია, ვიდრე GNSS მონაცემების. ასევე, თუ GPS მოდული გამორთულია ან მოწყობილობა დახურულ სივრცეშია, პრაქტიკულად გამოუსადეგარია GNSS ის მეთოდი. 5G ქსელის შემთხვევაში კი, როდესაც High-Band ზე იქნება მოწყობილობა, შესაძლებელია 1 ანძით დადგინდეს მისი მიახლოებითი მდებარეობა. ასევე ყურადსაღებია ის ფაქტი, რომ Fake Base Station ების შემთხვევაში, როდესაც მოწყობილობას ანძის არასწორი კოორდინატი შეიძლება მიეწოდოს, მისი LSB სერვისები გაუმართავად იმუშავებს. რამაც ზოგ შემთხვევაში შეიძლება სავალალო შედეგამდე მიგვიყვანოს.

5. დასკვნა

მეხუთე თაობის ქსელის დანერგვა და განვითარება მნიშვნელოვან როლს ითამაშებს კაცობრიობის სამომავლო განვითარებაში. რაც თავის მხრივ აისახება ეკონომიკურ ფაქტორებზეც. მასშტაბებიდან გამომდინარე ცდება ტელეკომ კომუნიკაციების იდეას და ქმნის ახალ ეკოსისტემას, სადაც გაერთიანებული იქნება სხვადასხვა ინდუსტრია, მათ შორის კრიტიკული სერვისები. აქედან გამომდინარე უპირობოდ მნიშვნელოვანია სტანდარტის უსაფრთხო იმპლემენტაცია. 5G ქსელს აქვს რიგი პრობლემები, როგორც წინა სტანდარტიდან გადმოყოლილი ასევე ახალი, ცვლილებებიდან/ფუნქციონალიდან გამომდინარე წარმოქმნილი საფრთხეები. კვლევის ეს ნაწილი მოიცავს ქსელის ერთ-ერთი ყველაზე მძლავრი შეტევის - MITM ის ანალიზს მეხუთე თაობის ქსელთან მიმართებაში და შედეგად გვაჩვენებს ამ პრობლემის მოგვარების ერთ-ერთ გზას, კონცეპტუალურ მოდელს. კვლევის შედეგად მიღებული შედეგების მიხედვით, თუ წინასწარ შეაფასებს მოწყობილობა არსებული ანძების დახმარებით სამიზნე ანძის ავთენტურობას, მაშინ მნიშვნელოვნად მცირდება ცრუ ანძების პრობლემა. არსებული დიზაინს, როგორც სხვა ნებისმიერ ფუნქციონალს, აქვს თავისი სისუსტეები - მაგალითად როუმინგი, როგორც შიდა ასევე გარე ქსელში. ამ კუთხით, როგორც დამზღვევი მექანიზმი შევიმუშავეთ წინასწარ განსაზღვრული ავტორიზებული ანძების სია, რომლის ეფექტურობაც დადასტურდა ჩვენსავე ჩატარებულ ექსპერიმენტში. ბუნებრივია, ეს არ ადასტურებს ჩვენი დიზაინის სრულ ეფექტურობასა და უსაფრთხოებას. ამის მისაღწევად აუცილებელია კვლევის გაგრძელება და რეალურ სისტემაზე დატესტვა. როგორც ექსპერიმენტულმა კვლევამ აჩვენა, MITM ს გამო დიდი საფრთხის ქვეშაა LBS სერვისები. ახალი არქიტექტურიდან გამომდინარე, შესაძლებელია High-Band ზე დაკავშირების შემთხვევაში 1 ანძით დადგინდეს მოწყობილობის მდებარეობა. MITM ის გამოყენებით კი A-GPS მეთოდის დროს მდებარეობა არასწორად გამოვათვლევინოთ მოწყობილობებს, რამაც შეიძლება მნიშნელოვანი ზიანი მიაყენოს კრიტიკულ ინფრასტრუქტურას და გადაუდებელ სერვისებს. შესაბამისად, 5G სერვისის ფართო მასშტაბებისთვის მიწოდებამდე, აუცილებელია საფრთხეების შემცირება

6. დადასტურება/აღიარება

კვლევა PHDF-21-088 განხორციელდა შოთა რუსთაველის საქართველოს ეროვნული სამეცნიერო ფონდის ფინანსური მხარდაჭერით

ბიბლიოგრაფია

1. Huawei Technologies CO,. LTD in “5G Network Architecture – A high Level Perspective”, 2016
2. S. Asad Hussain, S. Ahmed, M. Emran, “Positioning a Mobile Subscriber in a Cellular Network System based on Signal
Strength”, IAENG International Journal of Computer Science, 34:2, IJCS_34_2_13,2007.
https://www.researchgate.net/publication/26492533

3. Qualcomm Technologies inc. “What is 5G”, in online article. https://www.qualcomm.com/5g/what-is-5g
4. M. Hanif, “5G Phones Will Drain Your Battery Faster Than You Think”, in online journal, 2020. https://www.rumblerum.com/5g-phones-drain-battery-life/
5. A. Shaik, R.Borgaonkar, S. Park, J.P. Selfert. ” New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities” in WiSec ’19: Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, DOI: 10.1145/3317549, ISBN: 9781450367264, 2019.
6. Ultrasecurity, “Strom-Breaked” (Software Package), (Last access: 8.12.2021) https://github.com/ultrasecurity/Storm-Breaker
7. SK Telecom, in “5G architecture design and implementation guideline”, 2015.
8. Samsung in online report “Samsung Phone Battery Drains Quickly on 5G Service” https://www.samsung.com/us/support/troubleshooting/TSG01201462/
9. A. Purdy, “Why 5G Can Be More Secure Than 4G” in Forbes online journal, 2019. https://www.forbes.com/sites/forbestechcouncil/2019/09/23/why-5g-can-be-more-secure-than-4g/?sh=2ffcdf1657b2
10. Cell Phone Trilateration Algorithm, Online Journal “Computer Science”, 2019. (Last access: 10.12.2021) https://www.101computing.net/cell-phone-trilateration-algorithm/
11. Johhny, “How to find the Cell Id location with MCC, MNC, LAC and CellID (CID)”, 2015 https://cellidfinder.com/articles/how-to-find-cellid-location-with-mcc-mnc-lac-i-cellid-cid
12. M. Iavich, G. Akhalaia, S.Gnatyuk. Method of Improving the Security of 5G Network Architecture Concept for Energy and Other Sectors of the Critical Infrastructure, In: Zaporozhets A. (eds) Systems, Decision and Control in Energy III. Studies in Systems, Decision and Control, vol 399. Springer, Cham. https://doi.org/10.1007/978-3-030-87675-3_14,
13. M. K. Maheshwari, M.Agiwal, N. Saxena, R. Abhishek. "Flexible Beamforming in 5G Wireless for Internet of Things”, in IETE Technical Review, 36:1, 3-16, DOI: 10.1080/02564602.2017.1381048, 2017. https://doi.org/10.1080/02564602.2017.1381048
14. M. Ivezic, L. Ivezic, “5G Security & Privacy Challenges” in 5G.Security Personal Blog, 2019. https://5g.security/cyber-kinetic/5g-security-privacy-challenges/
15. Yusof, R., Khairuddin, U., and Khalid, M., ‘A New Mutation Operation for Faster Convergence in Genetic Algorithm Feature Selection’,In International Journal of Innovative Computing, Information and Control, Vol. 18, No. 10, 2012, pp 7363-7380.
16. Ibrahim S. Shehu, Olumide S, Adewale, Muhammad B.”Vehicle Theft Alert and Location Identification Using GSM, GPS and Web Technologies”, in I.J. Information Technology and Computer Sciences, 2016, 7, 1-7. Published Online July 2016 in MECS (http://www.mecs-press.org/)
17. The EU Space Programme (Last Access: 10.12.2021) https://www.euspa.europa.eu/european-space/eu-space-programme
18. Hu Z, R. Odarchenko, S. Gnatyuk “Statistical Techniques for Detecting Cyberattacks on Computer Networks Based on an Analysis of Abnormal Traffic Behavior”, in I.J. Computer Network and Information Security, 2020, 6, 1-13 Published Online December 2020 in MECS (http://www.mecs-press.org/)
19. M, Iavich, T. Kuchukhidze, S. Gnatyuk, “Novel Certification Method for Quantum Random Number Generators“, in I.J. Computer Network and Information Security, 2021, 3, 28-38 Published Online June 2021 in MECS (http://www.mecs-press.org/)
20. Avtandil Gagnidze, Maksim Iavich, Giorgi Iashvili// Novel Version of Merkle Cryptosystem// Bulletin of the Georgian National Academy of Sciences, vol. 11, no. 4, 2017, p. 28-33
21. Giorgi Iashvili, Zhadyra Avkurova, Maksim Iavich, Madina Bauyrzhan, Avtandil Gagnidze, Sergiy Gnatyuk// Content-Based Machine Learning Approach for Hardware Vulnerabilities Identification System// International Conference on Computer Science, Engineering and Education Applications // Springer, Cham, No 23 2021, p. 117 - 126