Scientific and Practical Cyber Security Journal (SPCSJ) 7(2): 1-6 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

მომხმარებლის მდებარეობის განსაზღვრა 5G ქსელში - High-Band ის გამოყენებით

LOCATING USER IN 5G NETWORKS USING HIGH-BAND

გიორგი ახალაია, საქართველოს ტექნიკური უნივერსიტეტი
Giorgi Akhalaia, georgian technical university

აბსტრაქტი: ბოლო წლებია ციფრულ ტექნოლოგიებსა და სერვისებში განსაკუთრებული ყურადღება ექცევა მომხმარებლის პერსონალური და მაიდენტიფიცირებელი ინფორმაციის უსაფრთხოებას. ახალი ფუნქციონალის, სერვისის დანერგვამდე, უსაფრთხოების ტესტირების პროცესში მუდმივი განხილვის საგანია მომხმარებლის პრივატულობა. მობილური ტექნოლოგიების, ხელოვნური ინტელექტის, ავტომატიზაციის სისტემების განვითარებამ, აუცილებელი გახადა მობილური კომუნიკაციების ახალი სტანდარტების დანერგვა. 3 მთავარი პრინციპით (ულტრა-საიმედო/დაბალი დაყოვნება; გაუმჯობესებული მობილური ბროუდბენდი; მანქანების მასიური რაოდენობით მიერთება), 5G სტანდარტი ცდება მობილური კავშირგაბმულობის ეკოსისტემას და და ქმნის უფრო მასშტაბურ ქსელს. გაუმჯობესებული დაცვის მექანიზმების მიუხედავად, 5G ქსელში ისევ რჩება სისუსტეები, რომლიდანაც თავდამსხმელს შეუძლია გარკვეული კიბერ შეტევების განხორციელება. MITM ტიპის შეტევით შესაძლებელი ხდება მომხმარებლის მოწყობილობის მოსმენა. კვლევის მიზანია 5G ქსელში არსებული საფრთხეების შეფასება მომხმარებლის პერსონალური მონაცემების უსაფრთხოებასთან მიმართებაში. ყურადღება გამახვილებულია მომხმარებლის მდებარეობის დადგენასთან დაკავშირებული საფრთხეების შეფასებაზე, 5G ქსელში არსებული სისუსტის გამოყენებით მომხმარებლის მდებარეობის დადგენაზე და მისგან თავის დაცვის რეკომენდაციების შემუშავებაზე.

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

ABSTRACT: In recent years, in digital technologies and services, special attention has been paid to the security of user's personal and personally identifiable information. Prior to the introduction of new functionality, the service, user privacy is a constant consideration during the security testing process. The development of mobile technologies, artificial intelligence, automation systems made it necessary to introduce new standards of mobile communications. With 3 key principles (ultra-reliability/low latency; improved mobile broadband; massive vehicle connectivity), the 5G standard will disrupt the mobile communications ecosystem and create a more scalable network. Despite the improved protection mechanisms, there are still weaknesses in the 5G network from which an attacker can carry out certain cyber attacks. A MITM type of attack makes it possible to eavesdrop on the user's device. The aim of the study is to assess the threats in the 5G network in relation to the security of the user's personal data. The focus is on assessing threats related to user location, using vulnerabilities in the 5G network to determine user location, and developing recommendations to protect against it.

KEYWORDS: *5G Network Security, Secure Communications; Location-Based Attacks, End-user privacy*

1. შესავალი

ტექნოლოგიურად განვითარებულმა და ძლიერი ეკონომიკის მქონე ქვეყნებმა ბოლო წლებში აქტიურად დანერგეს მეხუთე თაობის ქსელი. აშშ_სა და საქართველოს შორის 2021 წელს გაფორმდა მემორანდუმი. რომლის მიხედვითაც, ქვეყნებს მჭიდრო თანამშრომლობა ექნებათ და აშშ დაეხმარება საქართველოს როგორც 5G ქსელის დანერგვაში, ასევე მისი უსაფრთხოების უზრუნველყოფაში. მეხუთე თაობის ქსელის სამი KPIია:

- > 10Gb/s - (eMBB)
- > 1M/km²-(mMTC). ეს სიმჭიდროვე აღებულია IoT მოწყობილობებიდან გამომდინარე.
- < 1ms Latency - არაუმეტეს 1 მილიწამი დაყოვნება.(URLLC) [1]

ხოლო მეხუთე თაობის ქსელის სამუშაო სპექტრი, შემდეგნაირადაა დაგეგმილი:

1. **ქვედა არხი - (Low-band) -- < 1 GHz**
2. **შუა არხი - (Mid-band) -- 1 GHz – 6 GHz**
3. **მაღალი არხი - (High-band(mmWave)) – 6 GHz – 100 GHz**

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]

კვლევისას აქცენტი გაკეთებულია High-Band ის სიხშირეზე არსებული სისუსტის გამოყენებით შეტევის განხორციელებაზე და მომხმარებლის მდებარეობის დადგენაზე.

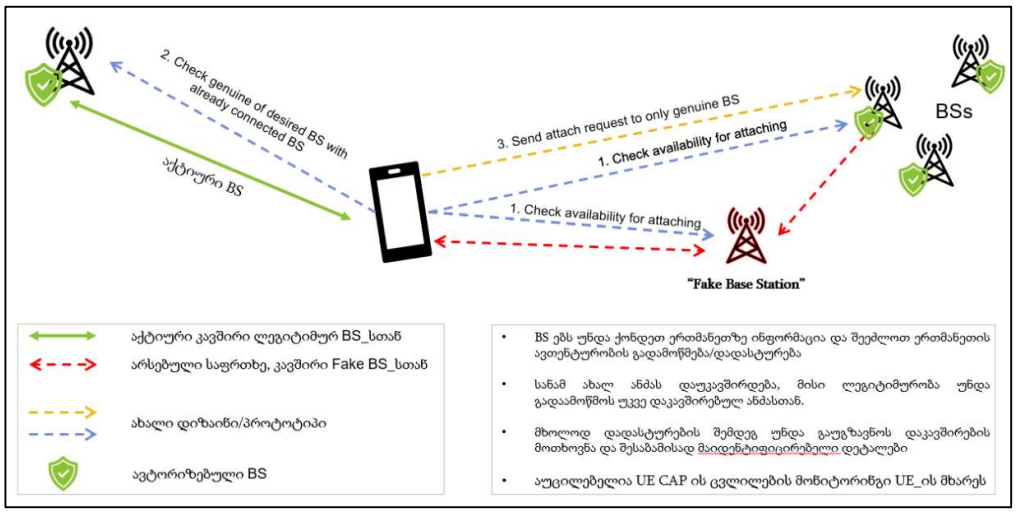
2. 5G_ს უსაფრთხოება

5G ქსელი თავისი არქიტექტურიდან, იდეიდან გამომდინარე კიდე უფრო კომპლექსურია. იქიდან გამომდინარე, რომ მეხუთე თაობის ქსელში ჩაირთვება სხვადასხვა მწარმოებლის, კატეგორიის, არქიტექტურისა და პროგრამული უზრუნველყოფის მქონე 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.

მართალია 4G_სგან განსხვავებით 5G ქსელი მომხმარებლის უსაფრთხოება შედარებით დახვეწილია, მაგრამ მაინც რჩება ინფორმაციის ნაწილი, რომელიც ე.წ. clear text_ად მიმოიცვლება ქსელში ბაზასთან დაკავშირებისას. 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. [5]

ამ ეტაპზე შემუშავებული დიზაინი, კვლევების თანახმად, მეხუთე თაობის ქსელი მოწყვლადია MITM ტიპის შეტევების მიმართ. რომელიც არის ერთ-ერთ ყველაზე ძლიერი შეტევა ქსელში. კვლევის შედეგად შევიმუშავეთ განახლებული, უსაფრთხო კონცეპტუალური დიზაინი, რომელიც მნიშვნელოვნად შეამცირებს ქსელში ე.წ. ცრუ ანძების ეფექტურობას.



ილუსტრაცია 1

ილუსტრაცია 1_ზე ნაჩვენებია განახლებული დიზაინის მიხედვით როგორ მოხდება მომხმარებლის მოწყობილობის ანძასთან დაერთება,

მოწყობილობის ლოკაციის განსაზღვრის 2 ძირითადი ტექნიკა, მეთოდი არსებობს: გლობალური სატელიტური სანავიგაციო სისტემა - GNSS ან A-GPS. GNSS გულისხმობს სატელიტების საშუალებით მოწყობილობის მდებარეობის დადგენას, A-GPS კი ოპერატორის ანძების გამოყენებით მომხმარებლის მოწყობილობის ლოკაციის გადათვლას/დაანგარიშებას. ორივე მეთოდს აქვს თავისი სუსტი მხარე და უპირატესობა: პირველის შემთხვევა (GNSS), მუშაობს ე.წ. ღია ცის პრინციპი, ანუ მოწყობილობას უნდა ქონდეს სატელიტების პირდაპირი ხედვა. მაგრამ ყველაზე დაბალ ცდომილებას იძლევა, ხოლო მეორე A-GPS, ოპერატორის მინიმუმ სამი ანძის მეშვეობით ითვლის თავის მდებარეობას. პირველ მეთოდთან შედარებით, ეს ნაკლებად ზუსტია, თუმცა, შეუძლია დახურულ სივრცეებშიც (შენობებში) განსაზღვროს მოწყობილობის კოორდინატები.

MITM ის შეტევის დროს, როდესაც ე.წ. “Fake Base Station“_ის ხდება, დიდია საფრთხე, რომ მოწყობილობის ლოკაცია არასწორად განისაზღვროს, რადგან თუ მიწოდებული მონაცემები არასწორია, შესაბამისად შედეგსაც არასწორს მივიღებთ. ეს კი დიდ საფრთხესა და პრობლემას უქმნის ე.წ. მდებარეობასთან დაკავშირებულ სერვისებს, მათ შორის გადაუდებელი სერვისებისთვის, როგორიცაა 911/112 საჭირო პროცესებს.

გამომდინარე იქიდან, რომ მოწყობილობა მუდმივად არ ითვლის თავის კოორდინატებს GPS გამოყენებით, პროგრამული უზრუნველყოფით ამ ტიპის ინფორმაციის მოპარვისას, მომხმარებელი ღებულობს გაფრთხილებას, რომ აპლიკაცია ცდილობს GPS მოდულის

გამოყენებას და მდებარეობის განსაზღვრას. უარყოფითი მხარეა ისიც, რომ თუ მოდული გამორთულია, ან მოწყობილობა შენობაშია, მაშინ არ იმუშავებს. ამ შემთხვევაში უფრო ეფექტურია, მომხმარებლის მოწყობილობიდან თუ A-GPS ის მონაცემებს წამოვიღებთ. დეტალური ინფორმაციის მიღება შეგვიძლია ანძების შესახებ, მათ შორის უნიკალური ID, სიგნალის სიძლიერე, კოორდინატები.

მოწყობილობამ რომ გამოიყენოს High-Band ანძები, ე.წ. mmWave, აუცილებელია რომ იმყოფებოდეს ანძასთანს ძალიან ახლოს, ე.წ. პირდაპირი ხედვით. გამომდინარე იქიდან, რომ ამ სიხშირეების ტალღებს ძალიან ამახინჯებს შენობები. შესაბამისად, ეს შეგვიძლია გამოვიყენოთ და 1 ანძითაც განვსაზღვროთ მოწყობილობის მდებარეობა. რაც დიდ საფრთხეს 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 დავაიდენტიფიცირეთ შეტევა, კერძოდ, შესაძლებელია მობილური ტელეფონის ანძასთან დაკავშირებისას გაგზავნილი, დაუშიფრავი „დაკავშირების მოთხოვნის“ გადამისამართება High-band ანძასთან. რომლის შემდეგაც ერთი ანძიცათ მოხერხდება მდებარეობის განსაზღვრა. ამისგან თავის დასაცავად შევიმუშავეთ ორი რეკომენდაცია:

- High-Band ანტენები არ უნდა ავრცელებდეს მაღალი სიზუსტის კოორდინატებს.
- მოწყობილობა არ უნდა უკავშირდებოდეს თავიდანვე high-band_ს. უნდა დაუკავშირდეთ ქვედა კატეგორიის ანძებს და მხოლოდ მათგან უნდა მოხდეს კავშირის გადამისამართება.

4. დასკვნა

მეხუთე თაობის ქსელის დანერგვა უპირობოდ მნიშვნელოვანია ქვეყნის ეკონომიკური განვითარებისთვის. მისი მასშტაბიდან გამომდინარე, აუცილებელია უსაფრთხოების მაღალ დონეზე უზრუნველყოფა. ბოლო პერიოდში განსკუთრებით ყურადღების ქვეშაა, მომხმარებლის პერსონალური ინფორმაცია. ნაშრომის ფარგლებში ჩატარებულმა კვლევებმა აჩვენა, რომ შესაძლებელია კიბერ შეტევით მეხუთე თაობის ქსელში მომხმარებლის მდებარეობის განსაზღვრა ერთი ანძითაც. შევიმუშავეთ ახალი, უსაფრთხო დიზაინი, რომლითაც შევამცირებთ MITM ის რისკს და ასევე ორი რეკომენდაცია, რომლითაც შეუძლებელს გავხდით ერთი ანძით ზუსტი მდებარეობის განსაზღვრას.

5. დადასტურება/აღიარება

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

6. 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
    a. Strength”, IAENG International Journal of Computer Science, 34:2, IJCS_34_2_13,2007.
    b. 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.
    a. https://www.rumblerum.com/5g-phones-drain-battery-life/
5. 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)
    a. 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”
    a. https://www.samsung.com/us/support/troubleshooting/TSG01201462/
9. Purdy, “Why 5G Can Be More Secure Than 4G” in Forbes online journal, 2019.
    a. 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)
    a. 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
    a. 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.
    a. 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.
        i. Published Online July 2016 in MECS (http://www.mecs-press.org/)
17. The EU Space Programme (Last Access: 10.12.2021)
    a. 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
    a. 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
    a. 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