Scientific and Practical Cyber Security Journal (SPCSJ) 5(1): 1-8 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

შეჭრის აღმოჩენის სისტემა 5G-სათვის

INTRUSION DETECTION SYSTEM FOR 5G

მაქსიმ იავიჩი, კავკასიის უნივერსიტეტი
Maksim Iavich, Caucasus University
გიორგი იაშვილი, კავკასიის უნივერსიტეტი
Giorgi Iashvili, Caucasus University
ავთანდილ გაგნიძე, კავკასიის უნივერსიტეტი
Avtandil Gagnidze, Caucasus University
შალვა ხუხაშვილი, სამეცნიერო კიბერ უსაფრთხოების ასოციაცია
Shalva Khukhashvili, Scientific Cyber Security Association
სერგეი სიმონოვი, სამეცნიერო კიბერ უსაფრთხოების ასოციაცია
Sergei Simonovi, Scientific Cyber Security Association

აბსტრაქტი

სატელეკომუნიკაციო ინდუსტრია მნიშვნელოვნად ვითარდება 5G ქსელების დასანერგად. ახალმა სტანდარტმა უნდა დააკმაყოფილოს ამჟამინდელი და მომავალი მომხმარებლების მოთხოვნები. მომხმარებლებსა და კლიენტებს ესაჭიროებათ მომსახურების უკეთესი ხარისხი და უსაფრთხოების მაღალი დონე, რათა უსაფრთხოდ გადაეცემოდეს მონაცემები და უხარვეზოდ მუშაობდეს სხვა შიდა სერვისები. შესაბამისად, წამყვანმა მობილურმა ოპერატორებმა უნდა უზრუნველყონ ბევრად უკეთესი სამომხმარებლო ხარისხი და უსაფრთხოება, ასევე უნდა გაუმჯობესდეს მათ მიერ შემოთავაზებული სერვისები. 5G-ს შემოთავაზებულ ახალ მეთოდიკას სჭირდება ქსელური, სერვისის დანერგვისა და მონაცემთა დამუშავების ახალი მიდგომები. აღნიშნულ მიდგომებს ახასიათებთ უსაფრთხოების გარკვეული ნაკლოვანებები, რაც ასევე კრიტიკული იქნება 5G ქსელებისთვის. ამ კუთხით მომუშავე მსოფლიოს წამყვანმა მკვლევარებმა უკვე საჯაროდ განაცხადეს 5G ქსელების ამჟამინდელ პრობლემებზე. ჩვენ მიერ წარმოდგენილი ანაზილი ცხადყოფს 5G-ს არსებული პრობლემების დეტალურ მიზეზებს, რაც შემტევს აძლევს საშუალებას სისტემაში ჩააშენოს მავნე კოდი და წარმატებით განახორციელოს შემდეგი შეტევები: MiTM, MNmap და Battery drain.

ჩვენ შევიმუშავეთ ახალი სისტემა შეტევების ამოსაცნობად, რომელიც დაფუძნებულია მანქანური და ღრმა დასწავლის უახლეს მეთოდებზე. ჩვენ ვთავაზობთ IDS-ის ინტეგრაციას 5G-ს არქიტექტურაში.

ABSTRACT

The telecommunications industry is evolving significantly to implement 5G networks. The new standard must meet the requirements of current and future users. Customers and clients need better quality of service and a high level of security in order for data to be transmitted securely and other internal services to work flawlessly. Consequently, leading mobile operators need to ensure much better customer quality and security, as well as improve the services they offer. The new methodology proposed by 5G requires new approaches to networking, service deployment, and data processing. These approaches are characterized by certain security vulnerabilities that will also be critical for 5G networks. The world's leading researchers working in this field have already publicly stated the current problems of 5G networks. Analysis presented by us reveals the detailed causes of 5G problems, which allows the attacker to install malicious code in the system and successfully carry out the following attacks: MiTM, MNmap and Battery drain.

We have developed a new system for detecting attacks based on the latest methods of machine and in-depth learning. We propose the integration of IDS into the 5G architecture.

საკვანძო სიტყვები: *5G ქსელი, 5G უსაფრთხოება, ფიჭური ქსელები*

KEYWORDS: *5G network, 5G security, cellular networks*

1. შესავალი

უსადენო ქსელებით გადაცემული ტრაფიკის რაოდენობა და მობილური მოწყობილობების რაოდენობა (IoT-ის ჩათვლით) არის ძალიან სწრაფად მზარდი, რაც გამოწვეულია რამდენიმე ფაქტორით. სატელეკომუნიკაციო ინდუსტრია განიცდის ძირითად ტრანსფორმაციას 5G ქსელების დასანერგად და მომხარებელთა არსებული და სამომავლო მოთხონილებების დასაკმაყოფილებლად. შესაბამისად, უსადენო 5G ქსელი მოიაზრება მონაცემთა გადაცემის ძალიან მაღალი სისწრაფის მქონედ და უკეთესი ხარისხის მქონედ, რაც გამყარებულია სიგნალის მიმღები სადგურების მჭიდრო განლაგების კონცეფციით, მომსახურების გაუმჯობესებული ხარისხით (QoS) და უკიდურესად მცირე შეყოვნებით. ყოველივე ზემოთქმულის განსახორციელებლად საჭიროა უახლესი ტექნოლოგიების დანერგვა და გამოყენება ქსელების, სერვისების, მარაგებისა და მონაცემთა დამუშავების მხრივ. ეს ტექნოლოგიები წარმოშობს ახალ გამოწვევებს 5G კიბერ უსაფრთხოების სისტემების ფუნქციონალობაში.

5G დააკავშირებს კრიტიკულ ინფრასტრუქტურებს, რისთვისაც საჭიროა მეტი დაცულობა არა მხოლოდ ინფრასტრუქტურის შიგნით, არამედ მთელ საზოგადოებაში. მაგალითად, უსაფრთხოების ხარვეზი ელექტროენერგიის კვების სისტემებში იქნება საზიანო გლობალურად და არა მხოლოდ რაიმე კერძო სექტორისათვის. შესაბამისად, აუცილებელია, რომ გამოვიკვლიოთ და აღმოვაჩინოთ მნიშვნელოვანი პრობლემები 5G ქსელებში და მოვიძიოთ უკვე არსებული გადაწყვეტილებები, რომლებიც აუმჯობესებს უსაფრთხოების ხარისხს. მკველვარები და დეველოპერები თავდაუზოგავად მუშაობენ ამ საკითხების

გამოსაკვლევად და იმისათვის, რომ 5G გახადონ უფრო დაცული. ქვემოთ მოვიყვანთ უკვე ცნობილ ხარვეზებს, რომლიც აქვს 5G-ს.

2. 5G-ს უსაფრთხოების პრობლემები

მკვლევარებმა აჩვენეს, რომ 5G-ს ჯერ კიდევ აქვს უსაფრთხოების პრობლემები[1-4]. ჩვენ გავაანალიზეთ და გამოვავლინეთ რიგი მიზეზებისა:

- 5G ქსელი არის დაუცველი პროგრამული უზრუნველყოფით განხორციელებული შეტევების მიმართ, აქვს ბევრი სუსტი ადგილი, რომლებსაც იყენებენ ჰაკერები. ამის მიზეზია ის, რომ მთლიანად სისტემა დიდწილად დაფუძნებულია პროგრამულ უზრუნველყოფაზე.
- იქიდან გამომდინარე, რომ 5G-ს ქსელურმა არქიტექტურამ მიიღო უფრო დიდი ფუნქცია, ქსელის სტრუქტურის გარკვეული ნაწილები იქნება გაცილებით მგრძნობიარე შეტევების მიმართ. საბაზო სადგურები და ქსელის გასაღების განაწილების ფუნქციები შეიძლება გახდეს ჰაკერების სამიზნე.
- ის ფაქტი, რომ მობილური ქსელების ოპერატორები დამოკიდებულები არიან მომმარაგებლებზე, შეიძლება გახდეს საფრთხის შემცველი, გაზარდოს შეტევისაგან მიყენებული ზიანი.
- ბევრი კრიტიკული IT აპლიკაცია გამოიყენებს 5G ქსელს, ამიტომ აპლიკაციის ხელმისაწვდომობა და მთლიანობა უსაფრთხოებისათვის საყურადღებო საკითხი იქნება.
- 5G ქსელში ჩართული ბევრი მოწყობილობის გამო, შეიძლება მნიშვნელოვნად გაიზარდოს DoS და DDoS ტიპის შეტევები.
- ქსელის შრეებად დაყოფა (Network Slicing) ასევე საყურადღებო საკითხია უსაფრთხოების მხრივ, რადგან შეიძლება შემტევმა იძულებით გამოაყენებინოს გარკვეულ მოწყობილობას შრე,სადაც მას არ აქვს დაშვების უფლება.

ბოლო წლებში, 5G-ს მკვლევარებმა აღმოაჩინეს სისუსტეები, რომელთა გამოყენებითაც შეიძლება მავნე კოდის ჩაყენება სისტემაში და მისი გამოყენება მომხმარებელთათვის საზიანო მიზნებისათვის. მაგალითად:

1. **MNmap**
   მკვლევართა გუნდა სნიფერით მოიპოვა ინფორმაცია, რომელიც ქსელში გაშვებული იყო დაუშიფრავად, ღია ტექსტის სახით. ამის მეშვეობით, მათ აღადგინეს მოწყობილობათა „რუკა“, რომლებიც მიერთებული იყო ამ ქსელთან. მეცნიერებმა შეძლეს დაედგინათ მოწყობილობის მწარმოებელი, მოდელი, ოპერაციული სისტემა და სხვა კერძო მახასიათებლები.

2. **MiTM**
   ახლანდელ 5G-ზე შეიძლება ასევე MiTM შეტევის განხორციელება. MiTM-ის გამოყენებით შეიძლება ასევე განხორციელდეს bidding-down დაbattery drain შეტევები. შემტევს შეუძლია მიმღები სადგურიდან ამოიღოს MIMO. ეს არის ნაწილი, რომელიც

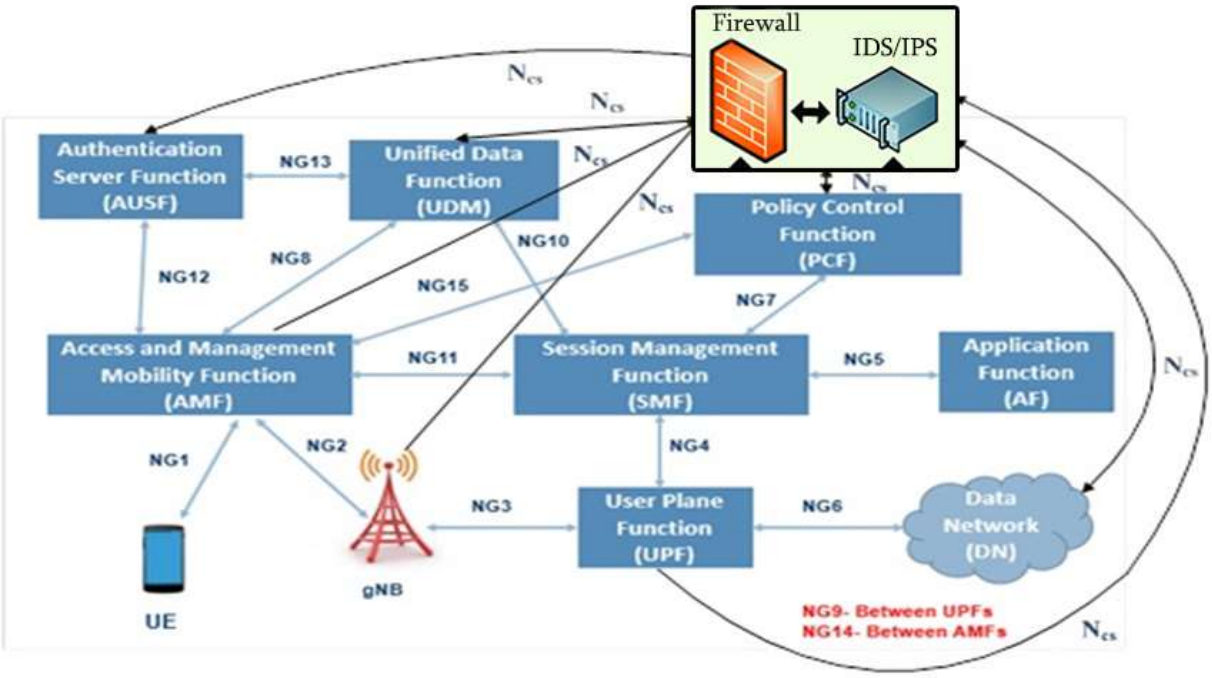
პასუხისმგებელია 5G-ს ძალიან მაღალ სიჩქარეზე. MIMO-ს გარეშე შეიძლება იგივე შეტევების განხორციელება, რაც ჩვეულებრივ ხდება 2G/3G ქსელებზე.

3. **Battery drain attack**
   ბატარეის გამოფიტვის შეტევა მიმართულია NB-IoT მოწყობილობებზე. ეს მოწყობილობები დროგამოშვებით აგზავნიან სიგნალებს და მოკლე ხანში შეიძლება დახარჯონ იმ რაოდენობის ენერგია, რაც ბატარეას ეყოფოდა 10 წელი PSM მდგომარეობაში. ჰაკერს შეუძლია ისე დაარეგულიროს PSM, რომ მსხვერპლი მიუერთდეს ჰაკერისათვის სასურველ ქსელს და გამოიყენოს მისი მოწყობილობა საზიანოდ.

ყოველივე ზემოთქმულის გათვალისწინებით, აუცილებელია ახალი არქიტექტურის შექმნა 5G და მომავალი 6G ქსელებისათვის, რათა ინტეგრირდეს უახლეს AI/ML კონცეფციებზე დაფუძნებული ალგორითმები, რაც ,თავის მხრივ, უზრუნველყოფს უსაფრთხოების უმაღლეს დონეს ყველა მისი მომხმარებლისათვის.

3. მეთოდოლოგია

ჩვენ ვთავაზობთ, რომ 5G-ს თითოეულ სადგურზე ჩაყენდეს კიბერ უსაფრთხოების ფუნქცია, როგორც დამატებითი სერვერი. ამ სერვერს ექნება Firewall და IDS/IPS. იდეა გრაფიკულად გამოსახულია ნახ.2-ზე.



ნახ. 2. კიბერ უსაფრთხოების ფუნქცია

ჩვენი კვლევიდან ჩანს, რომ 5G ქსელისათვის საფრთხის შემცველია Probe, DoS და პროგრამულ უზრუნველყოფასთან დაკავშირებული შეტევები. IDS-ის თავდაპირველი ვერსია დაფუძნებულია მანქანური სწავლების ალგორითმებზე. იმისათვის რომ IDS გაუმკლავდეს აღნიშნულ შეტევებს ის გავავარჯიშეთ შეტევების სხვადასხვა მონაცემების მიხედვით.

პირველი ბაზაა KDD99 [5-7]. ხაზგასასმელია ის ფაქტი, რომ აკადემიურ წრეებში IDS-ის პროტოტიპების შექმნისას მიღებულია KDD99-ის გამოყენება.

KDD99 არის ყველაზე ცნობილი მონაცემთა ნაკრები ანომალიების დასადგენად. ეს ბაზა შექმნილია DARPA'98 IDS პროგრამის ფარგლებში. ზემოხსენებული არის დაახლოებით 4 გიგაბაიტის ზომის პირველადი მონაცემები, რომელიც მიღებულია 7 კვირის განმავლობაში TCPDump-დან. 2 კვირის შესაბამისი მონაცემები შეიცავს დაახლოებით 2 მილიონ ჩანაწერს. მთლიანი ფაილი მოიცავს დაახლოებით 5 მილიონ ნიმუშს, რომლიც დაყოფილია როგორც შეტევა ან როგორც უსაფრთხო ტრაფიკი. ყველა შეტევა იყოფა 4 ძირითად ჯგუფად:

1) Denial of Service Attack (DoS): შეტევა, როდესაც იგზავნება ძალიან ბევრი მოთხოვნა, გადაივსება კომპიუტერის რესურსები და აღარ შეუძლია დააკმაყოფილოს მომხმარებლის მოთხოვნები.
2) User to Root Attack (U2R): შეტევის კლასი, როდესაც შემტევს ხელი მიუწვდება მომხმარებლის ლეგიტიმურ ანგარიშზე და შეუძლია ამ გზით შეაღწიოს შიდა სისტემაში,რის შედეგადაც მიიღებს სრულ წვდომას და გამოიყენებს შიგნით არსებულ სისუსტეებს.
3) Remote to Local Attack (R2L): შეტევის კლასი, როდესაც შემტევს არ აქვს ანგარიში კომპიუტერში, მაგრამ დისტანციურად შეუძლია გააგზავნოს პაკეტები და მიიღოს სრული წვდომა როგორც მომხმარებლი ლოკალურ კომპიუტერზე.
4) Probing Attack: შეტევა მიმართულია ქსელის შესახებ ინფორმაციის შეგროვებისაკენ, რათა გვერდი აუაროს უსაფრთხოების მექანიზმებს.

KDD-ს მთლიანი მონაცემები გაყოფილია გასავარჯიშებელ და გასატესტ შეტევის ტიპებად, შესაბამისად 24 და 14 მახასიათებელით.ეს მახასიათებლები შეიძლება გავყოთ 3 ჯგუფად:

1) ძირითადი მახასიათებლები: ყველა ინფორმაცია, რომელიც შეიძლება მივიღოთ TCP/IP კავშირის ანალიზის შედეგად. მათი აღმოჩენისას შეიძლება იყო პატარა შეყოვნება.
2) ტრაფიკის მახასიათებლები იყოფა 2 ჯგუფად:

2.1) "Same host" მახასიათებლები: მოწმდება ბოლო 2 წამში მომხდარი კავშირები, რომელთაც აქვთ იგივე მიმართულება (destination) რაც აქვს კონკრეტულ კავშირს. დამატებით ეს მახასიათებლები ითვლის სერვისის, პროტოკოლისა და სხვა სტატისტიკებს.

2.2) “Same service” მახასიათებლები: მოწმდება ბოლო 2 წამში მომხდარი კავშირები, რომლთაც აქვთ იგივე სერვისები რაც კონკრეტულ კავშირს. არსებობს შეტევების გარკვეული ტიპები, სადაც არ იყენებენ ინტერვალად 2 წამს და იყენებენ მაგალითად 1 წუთს. ამგვარი პრობლემის გადასაჭრელად, “same host” და“same service” მახასიათებლები მოწმდება ყოველ 100 კავშირზე.

3) კონტენტის მახასიათებლები: DoS და Probe შეტევები მოითხოვს მრავალ კავშირს მოკლე დროის განმავლობაში ერთსა და იმავე ჰოსტთან. თუმცა, R2L და U2R ტიპის შეტევები ამას არ საჭიროებენ. R2L და U2R შეტევები იგზავნება მონაცემთა პაკეტებთან ერთად და საჭიროებს მხოლოდ ერთ დაკავშირებას. ამ ტიპის შეტევების აღმოსაჩენად, ჩვენ უნდა გამოვიკვლიოთ საეჭვო ქმედებებები მონაცემთა კონკრეტულ პაკეტებში. მაგალითად: არასწორი პაროლის შეყვანის მცდელობათა რაოდენობა.

როგორც ვხედავთ, KDD99-ის მონაცემები იყოფა 4 ძირითად კატეგორიად: DOS, R2L, U2R და PROBE. DOS კატეგორია შეიცავს შემდეგ ქვეკატეგორიებს: APACHE2, PROCESSTABLE, UDPSTORM, BACK, LAND, NEPTUNE, POD, SMUR, MAILBOMB და TEARDROP. U2R კატეგორია შეიცავს შემდეგ ქვეკატეგორიებს: BUFFER_OVERFLOW, PS, SQLATTACK, XTERM, PERL, LOADMODULE, და ROOTKIT. R2L კატეგორია შეიცავს შემდეგ ქვეკატეგორიებს: FTP_WRITE, GUESS_PASSWD, HTTPTUNNEL IMAP, MULTIHOP, NAMED, SENDMAIL, SNMPGETATTACK, SNMGUESS, WXLOCK, XSNOOP, PHF, SPY, WAREZCLIENT და WAREZMASTER. ბოლო კატეგორია, PROBE, კი შეიცავს შემდეგ ქვეკატეგორიებს: IPSWEEP, NMAP, PORTSWEEP, NMA, MSCAN, SAINT და SATAN. R2L და U2R შეტევები მიმართულია პროგრამული უზრუნველყოფის სისუსტეებისადმი. შესაბამისად, IDS-ის დატრენინგება KDD-ს მონაცემებით 5G-სათვის არის ძალიან ხელსაყრელი, რადგან აღნიშნული შეტევები ფარავს 5G-სათვის კრიტიკული შეტევების აბსოლუტურ უმრავლესობას.

ასევე, ჩვენ დამატებით დავატრენინგეთ ჩვენი IDS DOS-ის შეტევების ორ ბაზაზე. პირველი შეიცავს ინფორაციას შემდეგ შეტევებზე: 'LDAP', 'MSSQL', 'NetBIOS', 'Syn', 'UDP', 'UDPLag' და მისი ზომაა 380 MB. მას აღვნიშნავთ DOS1-ით. მეორე კი შეიცავს მხოლოდ „Portmap“ შეტევას და არის 85 MB, მას აღვნიშნავთ როგორც DOS2. აღსანიშნავია, რომ მონაცემები არის საკმაოდ დიდი მოცულობის.

ჩვენ გავყავით KDD99-ის მონაცემები სატესტო და გასავარჯიშებელ ნაწილებად. სატესტო ნაწილი არის მთლიანი ბაზის 10%, გასავარჯიშებელი კი - 90%. იგივე პროცედურა ჩავატარეთ DOS1 და DOS2 ფაილებზე, გავყავით 20%-80% შესაბამისი თანაფარდობით. ასეთი განაწილება გვაძლევს შეტევის ამოსაცნობი სიზუსტის ძალიან მაღალ მაჩვენებელს. KDD99-ის შემთხვევაში არის 0.9611049372916336, DOS1-ის შემთხვევაში არის 0.9937894736842106, ხოლო DOS2-ის შემთხვევაში კი - 0.9998956703182055.

გავარჯიშების შემდეგ, მოდელი ელოდება მონაცემებს ქსელის სნიფერისგან. თავდაპირველად, მონაცემები მოწმდება შედის თუ არა KDD99-ში. თუ შეტევა იდენტიფიცირდება, გადაეცემა IPS-ს (შეღწევისგან დასაცავ სისტემას). თუ შეტევა არაა იდენტიფიცირებული, შემდეგ ავტომატურად გადაეცემა DOS1-ის მონაცემებში შესამოწმებლად, ინდენტიფიცირების შემთხვევაში გდაეცემა IPS-ს. წინააღმდეგ შემთხვევაში,

ავტომატურად მოწმდება DOS2-ის მონაცემებში და იდენტიფიცირებისას გადაეცემა IPS-ს. თუ IDS მაინც ვერ დაადგენს შეტევას, აღნიშნული ტრაფიკი ჩაითვლება უსაფრთხოდ და გააგრძელებს შემდეგი მონაცემების დამუშავებას ზემოაღნიშნული ეტაპებით.

4. დასკვნა

ზემოთ აღწერილი 5G-ს კიბერ უსაფრთხოების ფუნქცია, გავარჯიშებულია შეტევების აბსოლუტურ უმრავლესობაზე, რომელსაც შეუძლია გატეხოს ახლანდელი 5G სისტემა. ჩვენი მიდგომა არსებითად განსხვავებულია ამ მიმართულებაში უკვე არსებული მიდგომებისგან. სხვა სტატიებში IDS-ს ძირითადად ავარჯიშებენ მხოლოდ KDD99-ის მონაცემებით, თუმცა ჩვენს მოდელში KDD99 გამოყენებულია ერთ-ერთ მონაცემთა ბაზად, გარდა ამისა ვიყენებთ სხვა ტიპის შეტევების შემცველ მონაცემთა ბაზებსაც. ჩვენი ჩატარებული ექსპერიმენტებიდან ჩანს, რომ აღნიშნულ მოდელს შეუძლია ამოიცნოს განხორციელებული შეტევების აბსოლუტური უმრავლესობა.

ამ დროისათვის მიღებული ექსპერიმენტალური შედეგები არის საწყისი და ჩვენ ვმუშაობთ სატესტო ლაბორატორიის განვითარებაზე, რათა შევქმნათ მაქსიმალურად ზუსტი და კომპლექსური შეტევის ვექტორები. ამის შემდეგ, ჩვენი მიზანი იქნება შეტევების საკუთარი მონაცემების დაგენერირება ჩვენს სატესტო ლაბორატორიაში და IDS-ის გავარჯიშება ახალი მონაცემებით. ხოლო შემდეგ კი, დავიწყებთ IDS-ის ტესტირებას რეალური 5G გარემოში.

5. Acknowledgment

აღნიშნული კვლევა დაფინანსებულია შოთა რუსთაველის ეროვნული სამეცნიერო ფონდის

მიერ და განხორციელდა PHDF-19-519 გრანტის ფარგლებში.

ბიბლიოგრაფია

1. The analysis of the difference of 4G and 5G securities; M. Iavich, G. Iashvili, A. Gagnidze, L. Nachkebia, S. Khukhashvili; Scientific and practical cyber security journal, (SPCSJ) 4(3); 2020.
2. Y. Sun, Z. Tian, M. Li, C. Zhu and N. Guizani, "Automated Attack and Defense Framework toward 5G Security," in *IEEE Network*, vol. 34, no. 5, pp. 247-253, September/October 2020, doi: 10.1109/MNET.011.1900635.
3. Park S., Cho H., Park Y., Choi B., Kim D., Yim K. (2020) Security Problems of 5G Voice Communication. In: You I. (eds) Information Security Applications. WISA 2020. Lecture Notes in Computer Science, vol 12583. Springer, Cham. https://doi.org/10.1007/978-3-030-65299-9_30
4. LIU Jianwei, HAN Yiran, LIU Bin, YU Beiyuan. Research on 5G Network Slicing Security Model[J]. Netinfo Security, 2020, 20(4): 1-11.

5. Ullah I., Mahmoud Q.H. (2020) A Scheme for Generating a Dataset for Anomalous Activity Detection in IoT Networks. In: Goutte C., Zhu X. (eds) Advances in Artificial Intelligence. Canadian AI 2020. Lecture Notes in Computer Science, vol 12109. Springer, Cham. https://doi.org/10.1007/978-3-030-47358-7_52
6. Ullah I., Mahmoud Q.H. (2020) A Scheme for Generating a Dataset for Anomalous Activity Detection in IoT Networks. In: Goutte C., Zhu X. (eds) Advances in Artificial Intelligence. Canadian AI 2020. Lecture Notes in Computer Science, vol 12109. Springer, Cham. https://doi.org/10.1007/978-3-030-47358-7_52
7. Kumar, V., Sinha, D., Das, A.K. *et al.* An integrated rule based intrusion detection system: analysis on UNSW-NB15 data set and the real time online dataset. *Cluster Comput* **23,** 1397–1418 (2020). https://doi.org/10.1007/s10586-019-03008-x