უსაფრთხოების ახალი ტექნოლოგიები 6G ქსელებისთვის

რამაზ ხუროძე
ტექნიკურ მეცნიერებათა დოქტორი, პროფესორი,
საქართველოს მეცნიერებათა ეროვნული აკადემიის აკადემიკოსი

სერგო შავგულიძე
ტექნიკურ მეცნიერებათა დოქტორი, პროფესორი,
საქართველოს ტექნიკური უნივერსიტეტი

მამუკა ჩხაიძე
აკადემიური დოქტორი, ასოცირებული პროფესორი,
საქართველოს ტექნიკური უნივერსიტეტი

საქართველოს ტექნიკური უნივერსიტეტი

თბილისი 2022

რამაზ ხუროძე, სერგო შავგულიძე, მამუკა ჩხაიძე
უსაფრთხოების ახალი ტექნოლოგიები 6G ქსელებისთვის
Ramaz Khurodze, Sergo Shavgulidze, Mamuka Chkhaidze
New Security Technologies for 6G Networks

წინამდებარე წიგნში შესწავლილია უსაფრთხოების ახალი ტექნოლოგიები 6G ქსელებისთვის, რომელიც მომზადებულია უახლეს პუბლიკაციებსა და სამეცნიერო მიღწევებზე დაყრდნობით. განხილულია 6G ქსელების უსაფრთხოებასთან დაკავშირებული ტექნოლოგიური ტენდენციები, საფრთხეები, გადაწყვეტილებები და ფიზიკური ფენის უსაფრთხოების როლი კონტექსტით გაცნობიერებული უსაფრთხოებისთვის 6G ქსელებში. შესწავლილია მოძრავი სამიზნეების დაცვა, როგორც პროაქტიული თავდაცვის ელემენტი B5G სისტემებისთვის, ენერგოეფექტიანობის თვალსაზრისით ადაპტიური და დინამიკური უსაფრთხოება ხელოვნური ინტელექტის შემცველ 6G ქსელებში. შესწავლილია უსაფრთხოების ფუნქციის ვირტუალიზაცია საგნების ინტერნეტის აპლიკაციებისთვის 6G ქსელებში, ხოლო საგნების ინდუსტრიული ინტერნეტის კუთხით წარმოდგენილია ღრმა სწავლებაზე დაფუძნებული საფრთხის გამოვლენა, რაც კრიტიკული ინფრასტრუქტურის დაცვას და ბლოკჩეინზე დაფუძნებული, სანდო იდენტიფიკატორით ერთობლივი მმართველობის არქიტექტურას შეუწყობს ხელს. ასევე განხილულია უსაფრთხო ვირტუალური მობილური პატარა ფიჭები და ზონდირების, კომუნიკაციისა და უსაფრთხოების ინტეგრირება, როგორც შესაბამისი ნაბიჯები მრავალფუნქციური 6G ქსელებისკენ. წიგნი წარმოგვიდგენს ამ მიმართულებებით ბოლოდროინდელი მიღწევების სისტემურ განხილვას, შესაძლო გამოწვევებს და კვლევით მიმართულებებს, რომლებიც 6G მობილური უსადენო ქსელების უსაფრთხოების პრობლემების გადაჭრას შეუწყობს ხელს. ვფიქრობთ, რომ მასალა სასარგებლო იქნება და დახმარებას გაუწევს საინფორმაციო ტექნოლოგიებისა და კომუნიკაციების დარგში მომუშავე სპეციალისტებს, აკადემიურ პერსონალს, ბაკალავრიატის მაღალი კურსის სტუდენტებს, მაგისტრანტებსა და დოქტორანტებს.

რედაქტორი – ლიკა ქაჯაია
კორექტორი – რუსუდან გელაშვილი
დამკაბადონებელი – დათო მოსიაშვილი

ნაშრომი შესრულებულია შოთა რუსთაველის საქართველოს ეროვნული სამეცნიერო ფონდის ფინანსური მხარდაჭერით (გრანტის ნომერი FR-19-105).

დამტკიცებულია მონოგრაფიად საქართველოს ტექნიკური უნივერსიტეტის სარედაქციო-საგამომცემლო საბჭოს მიერ: 01.11.2022, ოქმი № 3.

ISBN 978-9941-8-4998-5

შინაარსი

წინასიტყვაობა 6

თავი 1. 6G ქსელების უსაფრთხოებასთან დაკავშირებული ტექნოლოგიური ტენდენციები და გადაწყვეტილებები

1.1. შესავალი 11
1.2. ტექნოლოგიური ტენდენციებიდან გამომდინარე 6G-ის წინაშე მდგარი უსაფრთხოების პრობლემები 13
1.2.1. ღიაობით გამოწვეული საფრთხეები 14
1.2.2. შეჯიბრებითი მანქანური სწავლებით გამოწვეული საფრთხეები 15
1.2.3. კონფიდენციალურობის საფრთხეები 17
1.2.4. ვირტუალიზაციის/კონტეინერიზაციის საფრთხეები 17
1.2.5. კვანტური გამოთვლების დანერგვით გამოწვეული საფრთხეები 18
1.3. გზა 6G-ის უსაფრთხოების მიმართულებით: გადაწყვეტილებები სანდოობისთვის 19
1.3.1. ღიაობასთან დაკავშირებული გადაწყვეტილებები 19
1.3.2. AI უსაფრთხოების ტექნოლოგიები 21
1.3.3. კონფიდენციალურობის შემანარჩუნებელი გადაწყვეტილება 22
1.3.4. გადაწყვეტილება ვირტუალიზაციის/კონტეინერიზაციის უსაფრთხოებისთვის 22
1.3.5. პოსტკვანტური კრიპტოგრაფიის დანერგვა 23
1.4. პირველი თავის დასკვნა 23

თავი 2. კონტექსტით გაცნობიერებული უსაფრთხოება და უსაფრთხოების ხარისხის კონტროლი 6G ქსელებისთვის

2.1. შესავალი 24
2.2. 5G უსაფრთხოების ღია საკითხები და უსაფრთხოების კვლევების გამოწვევები 6G-სთვის 25
2.3. 6G, როგორც კონტექსტით გაცნობიერებული QoSec-ის დანერგვის საშუალება PLS-ის გამოყენებით 27
2.4. QoSec ადაპტიური უსაფრთხოების კონტროლი: ფიზიკური ფენის უსაფრთხოების როლი 6G-ში 31
2.5. დისკუსია და შემოთავაზებული გზამკვლევი რუკა 34
2.6. მეორე თავის დასკვნა 35

თავი 3. მოძრავი სამიზნეების დაცვა და მისი ინტეგრირება B5G სისტემების უსაფრთხოების არქიტექტურაში

3.1. შესავალი 37
3.2. ჩატარებული კვლევების მიმოხილვა და ტექნიკური საფუძვლები 38
3.3. MTD-ის ინტეგრირება B5G სისტემებში სხვადასხვა დონეზე 40
3.4. სტანდარტიზაციის აქტივობები და მომავლის პერსპექტივა 43
3.4.1. ინტეგრირება NFV უსაფრთხოების არქიტექტურაში 44
3.4.2. MTD-ის ღირებულებასა და ეფექტიანობას შორის კომპრომისი 45

3.5. გამოწვევები და მომავალი კვლევის მიმართულებები 46
3.5.1. არქიტექტურული გამოწვევები....46
3.5.2. გამოწვევები 6G აპლიკაციებისა და მოთხოვნების გამო 47
3.5.3. AI/ML-თან დაკავშირებული გამოწვევები 48
3.5.4. ორკესტრირება და მენეჯმენტის გამოწვევები 49
3.6. მესამე თავის დასკვნა....49

თავი 4. ადაპტიური და დინამიკური უსაფრთხოება ხელოვნური ინტელექტის შემცველ ენერგოეფექტიან 6G ქსელებში
4.1. შესავალი....50
4.2. 6G-ის არქიტექტურისა და ხედვების მიმოხილვა....51
4.3. გამოწვევები 6G-ის უსაფრთხოების კუთხით 54
4.3.1. წარმოქმნილი საფრთხეები 54
4.3.2. უსაფრთხოების საკითხები ენერგეტიკული თვალსაზრისით....56
4.4. ოპტიმიზაციის სტრუქტურა უსაფრთხოებასა და ენერგეტიკას შორის კომპრომისისთვის 58
4.4.1. შემოთავაზებული სტრუქტურის მიმოხილვა....58
4.4.2. უსაფრთხოების ოპტიმიზაცია სხვადასხვა სცენარისთვის 61
4.4.3. კომპიუტერული სიმულაციის შედეგები....62
4.5. 6G-ის უსაფრთხოების ღია საკითხები....63
4.6. მეოთხე თავის დასკვნა 65

თავი 5. უსაფრთხოების ფუნქციის ვირტუალიზაცია საგნების ინტერნეტის მოწყობილობებისთვის 6G ქსელებში
5.1. შესავალი....66
5.2. ჩატარებული კვლევების მოკლე მიმოხილვა....68
5.3. ქსელის მოდელი და შემოთავაზებული სტრუქტურა....70
5.3.1. დისტანციური ატესტაცია....71
5.3.2. ქსელის იზოლაციის დონეები....72
5.3.3. სტრუქტურის მუშაობა 73
5.4. მახასიათებლების ანალიზი....74
5.4.1. ძირითადი მიზნები 74
5.4.2. მავნე პროგრამების კონტროლი 74
5.5. მეხუთე თავის დასკვნა....77

თავი 6. ღრმა სწავლებაზე დაფუძნებული საფრთხეების გამოვლენის სქემა საგნების ინდუსტრიული ინტერნეტისთვის
6.1. შესავალი....78
6.2. APT თავდასხმების აღწერა IIoT-ში....79
6.3. ღრმა სწავლებაზე დაფუძნებული, APT-ის პროაქტიული გამოვლენა IIoT-ში 81
6.3.1. APT თავდასხმების მიმდევრობის ანალიზი 82
6.3.2. APT თავდასხმის სიტყვის ვექტორის გენერაცია....83
6.3.3. წინასწარი ტრენინგის BERT ენის მოდელი 84

6.3.4. თავდასხმების მიმდევრობის ოპტიმიზაცია IIoT-ში 85
6.3.5. BERT-ზე დაფუძნებული APT თავდასხმის გამოვლენის ალგორითმი 86
6.4. ექსპერიმენტული ანალიზი....86
6.5. მეექვსე თავის დასკვნა....89

თავი 7. ბლოკჩეინზე დაფუძნებული სანდო იდენტიფიკატორით მმართველობის სტრუქტურა საგნების ინდუსტრიული ინტერნეტისთვის

7.1. შესავალი....90
7.2. დაკავშირებული კვლევითი სამუშაოები....91
7.3. სანდო იდენტიფიკატორით ერთობლივი მმართველობის არქიტექტურა 94
7.4. სანდო იდენტიფიკატორით ერთობლივი მმართველობის არქიტექტურის განხორციელების მეთოდები 96
7.5. ექსპერიმენტული შედეგები, დისკუსიები და ღია საკითხები....99
7.6. მეშვიდე თავის დასკვნა....102

თავი 8. უსაფრთხო ვირტუალური მობილური პატარა ფიჭების შემუშავება B5G/6G ქსელებისთვის

8.1. შესავალი....103
8.2. SECRET-ის ხედვა: მობილური პატარა ფიჭები B5G-სთვის 104
8.3. მობილური პატარა ფიჭების შემუშავება ქსელის ვირტუალიზაციისა და SW-ის საშუალებით 106
8.4. უსაფრთხოების უზრუნველყოფა მობილური პატარა ფიჭებისთვის 109
8.5. მწვანე RF SECRET-ით მხარდაჭერილი ტელეფონებისთვის....111
8.6. მობილური პატარა ფიჭების დემონსტრირება: SECRET-ის საცდელი სტენდი 112
8.7. მობილური პატარა ფიჭების სტანდარტიზაცია 113
8.8. მერვე თავის დასკვნა....115

თავი 9. ზონდირების, კომუნიკაციების და უსაფრთხოების ინტეგრირება 6G ქსელებში

9.1. შესავალი....116
9.2. ISAC-ის საფუძვლები....117
9.3. უსაფრთხოების ინტეგრირება ISAC-ში....119
9.4. ღია გამოწვევები და მომავალი სამუშაო....123
9.5. მეცხრე თავის დასკვნა....124

ბოლოთქმა....126
ლიტერატურა....127
აბრევიატურები და აკრონიმები....134

წინასიტყვაობა

უსაფრთხოება არის ნებისმიერი საკომუნიკაციო ქსელის ერთ-ერთი ყველაზე მნიშვნელოვანი ასპექტი, მაგრამ ის ასევე არის ერთ-ერთი ყველაზე დაუფასებელი და ნაკლებად შესწავლილი საკითხი. უსადენო ქსელებში, დიზაინის მთავარი აქცენტი, როგორც წესი, არის მონაცემთა გადაცემის სიჩქარე და უსაფრთხოების მოთხოვნა მეორეხარისხოვანი ხდება. იმ ეპოქაში, სადაც საზოგადოების დიდი ნაწილი ხანგრძლივ დროს ატარებს ინტერნეტში, დაბალი დონის უსაფრთხოების გამო შესაძლოა გამჟღავნდეს მგრძნობიარე პერსონალური ინფორმაცია, დაწყებული ინდივიდუალური პრეფერენციებიდან საბანკო ანგარიშის დეტალებამდე.

ფიჭურ ქსელებში უსაფრთხოების დაცვა შეიძლება რთული ამოცანა იყოს. მიუხედავად იმისა, რომ ფიჭური ქსელები შედარებით უსაფრთხოა, ჩვენ არ უნდა დავივიწყოთ, რომ ფიჭური ლინკები ქმნიან თავდასხმის ზედაპირს, რომელიც ჰაკერებს შეუძლიათ გამოიყენონ. მეხუთე თაობის (5G) ფიჭური ქსელების მთავარი ნაკლი არის ის, რომ უსაფრთხოებისა და კონფიდენციალურობის პრობლემები ჯერ კიდევ გადაუჭრელია. ამ მნიშვნელოვანი საკითხის გათვალისწინებით, ეს წიგნი მიზნად ისახავს შეისწავლოს უსაფრთხოების სისტემები, რომლებიც შეიძლება გამოიყენონ მომავალ მეექვსე თაობის (6G) უსადენო ქსელებში და გამოავლინოს ხარვეზები შესაბამის ტექნოლოგიებში, რომლებიც საჭიროებს შემდგომ კვლევას.

წინამდებარე წიგნში, რომელიც მიმოხილვითი ხასიათისაა, გრძელდება საუბარი 6G-ის თემატიკასთან დაკავშირებულ კვლევის შედეგებზე, რაც უახლეს პუბლიკაციებსა და სამეცნიერო მიღწევებზე დაყრდნობითაა მომზადებული. ამასთან, ეს წიგნი განსხვავდება ქართულ ენაზე გამოცემული, 6G-სადმი მიძღვნილი წინა წიგნებისგან და ავსებს მათ. საქმე ისაა, რომ ბოლო პერიოდში 6G ქსელების უსაფრთხოების მიმართულებით ძალიან ბევრი საინტერესო და სერიოზული საჟურნალო პუბლიკაცია გახდა ხელმისაწვდომი. გადავწყვიტეთ, ჩვენი აზრით საუკეთესო ნაშრომები შეგვეკრიბა (ყველა მათგანი მოცემულია წიგნის ბოლოს მითითებულ ლიტერატურაში), მოგვეხდინა მათი სისტემატიზაცია და ერთიან სტრუქტურაში გაერთიანება, ქართულ ენაზე წარმოგვედგინა ამ ნაშრომებში მოყვანილი ძირითადი შედეგები და დაგვეწერა ეს წიგნი. შეზღუდული ფორმატის გამო, ავარჩიეთ მხოლოდ რამდენიმე პერსპექტიული მიმართულება, რომლებიც მოიცავს 6G უსაფრთხოების სხვადასხვა ასპექტს და რომლებიც თავების მიხედვით შეჯამებულია შემდეგნაირად:

6G-ის მიმართულებით მიმავალ გზაზე ჩვენ მოწმენი ვართ სხვადასხვა ტექნოლოგიური ტენდენციების, რომლებიც მოიცავს ქსელის ღიაობას და ღია წყაროს პროგრამულ უზრუნველყოფაზე (SW) დაფუძნებულ მობილურ საკომუნიკაციო სისტემებს, ქსელურ ხელოვნურ ინტელექტს (AI), კონფიდენციალურობის დაცვას, ვირტუალიზაციასა და კონტეინერიზაციას, ასევე, კვანტურ გამოთვლებს. მოსალოდნელია, რომ ეს ტენდენციები უსაფრთხოებასთან დაკავშირებულ ახალ პრობლემებს გამოიწვევს. ქსელის არქიტექტურის ღიაობამ და ღია წყაროს ფართო გამოყენებამ შესაძლოა სისტემაში თავდასხმის შესაძლებლობები გაზარდოს. თავდამსხმელმა შეიძლება სცადოს AI-ზე დაფუძნებული რადიოწვდომის ქსელის ან ძირითადი ქსელის მოტყუება, რათა გამოიწვიოს გაუმართაობა შეჯიბრებითი მანქანური სწავლების (AML) მეთოდების გამოყენებით. პერსონალიზაციის ტექნოლოგია 6G-ში ასევე აღებს კარს კონფიდენციალურობაში მცირემასშტაბიანი შეჭრისთვის. ვირტუალიზაციისა და კონტეინერიზაციის დანერგვას ასევე შემოაქვს თავდასხმის ახალი გზა და მოსალოდნელია, რომ კვანტური გამოთვლების დანერგვა გავლენას მოახდენს არსებული კრიპტოგრაფიული ალგორითმების უსაფრთხოებაზე, რომლებიც დღევანდელ მობილურ ქსელებში გამოიყენება. შესაბამისად, **პირველ თავში** ჩვენ ვაანალიზებთ

ამ ახალ პოტენციურ საფრთხეებს, რომლებიც გამოწვეულია ახალი ტექნოლოგიების დანერგვით და წარმოვადგენთ შესაძლო მიდგომებს ამ საფრთხეების თავიდან ასაცილებლად.

მოსალოდნელია, რომ 6G სისტემები შეეჯახებიან უსაფრთხოების ახალ გამოწვევებს და ამავდროულად გახსნიან ახალ საზღვრებს კონტექსტის გასაცნობიერებლად უსადენო პერიფერიაზე. ამ დაგეგმილი ტექნოლოგიური ნახტომის განმახორციელებელი ძალა იქნება 6G მოწყობილობებისთვის ნაწინასწარმეტყველები ზონდირების შესაძლებლობების სრულიად ახალი ნაკრები, გარდა პერიფერიული მოწყობილობებისა და მათში ჩაშენებული ინტელექტისა. ამ მოწინავე ფუნქციების ერთობლიობამ შეიძლება გამოიწვიოს ახალი თაობის ადაპტირებული და კონტექსტური უსაფრთხოების პროტოკოლების შექმნა, რომლებიც შეესაბამება უსაფრთხოების ხარისხის (QoSec) პარადიგმას. ამ მოწინავე მახასიათებლების კომბინაციამ შეიძლება მიგვიყვანოს ადაპტიური და კონტექსტით გაცნობიერებული უსაფრთხოების პროტოკოლების ახალ სახეობამდე, უსაფრთხოების ხარისხის პარადიგმის მიხედვით. ამ სტრუქტურაში, ფიზიკური ფენის უსაფრთხოების გადაწყვეტილებები ხდებიან კონკურენტუნარიანი კანდიდატები, დაბალი სირთულის, დაბალი შეყოვნების, მცირე კვალის, ადაპტიური, მოქნილი და კონტექსტით გაცნობიერებული უსაფრთხოების სქემებისთვის, რომლებიც იყენებენ ფიზიკურ ფენას და პირველად შემოჰყავთ უსაფრთხოების მართვის ელემენტები ყველა ფენაზე, რაც განხილულია **მეორე თავში**.

6G ქსელები 5G-ის მიერ შემოთავაზებულ ციფრულ სერვისებს სრულიად ახალ დონეზე აიყვანს, მნიშვნელოვნად გაზრდილი მონაცემთა გადაცემის სიჩქარით, დაბალი შეყოვნებით და ულტრა მაღალი საიმედოობით. თუმცა, ამ სისტემების უსაფრთხოება გადამწყვეტია 6G-ის დაპირებების შესასრულებლად. ამ მოთხოვნის კრიტიკული ელემენტია 6G ინფრასტრუქტურისა და სერვისების ეფექტიანი, ყოვლისმომცველი დაცვა. მოძრავი სამიზნეების დაცვა (MTD) არის სისტემის მრავალ განზომილებაში ცვლილების მართვის კონცეფცია, რათა გაზარდოს გაურკვევლობა და აღქმული სირთულე თავდამსხმელებისთვის, შეამციროს მათი შესაძლებლობების ფანჯარა და გაზარდოს მათი ძალისხმევა მიმართული საძიებო და თავდასხმის ოპერაციებისადმი. **მესამე თავში** ჩვენ განვიხილავთ MTD-ის, როგორც ძირითად პროაქტიულ თავდაცვის ელემენტს და შევისწავლით, თუ როგორ შეიძლება მისი ინტეგრირება 5G-ის შემდგომ (B5G) შემუშავებულ სისტემებში. ასევე წარმოვადგენთ სტანდარტიზაციის პერსპექტივას, შესაბამის კვლევით გამოწვევებს და სამომავლო კვლევების მიმართულებებს.

AI-ზე დაფუძნებული ახალი სერვისები და ტექნოლოგიები, როგორიცაა დაკავშირებული მანქანები, ინტელექტუალური ინდუსტრია და ჭკვიანი ქალაქები, გაჩნდება 6G ფიჭურ ქსელთან ერთად ყოველდღიური ცხოვრების, მრეწველობისა და საზოგადოების სარგებლიანობისათვის. თუმცა, 6G ქსელის მზარდი ინტეგრაცია ფიზიკურ სამყაროსთან იწვევს ბევრ ახალ სცენარს, რაც ახალ გამოწვევებს უქმნის 6G-ის, განსაკუთრებით უსაფრთხოებისა და ენერგეტიკის კუთხით. 5G ქსელებში უსაფრთხოების გადაწყვეტილებები ყველა მოწყობილობასა და საბაზო სადგურზე კონფიგურირებულია უნივერსალური პარამეტრებით გარკვეული ტიპის თავდასხმებისთვის. ეს ერთჯერადი სტრატეგია აღარ არის შესაფერისი 6G უსაფრთხოებისთვის, მოწყობილობის შესაძლებლობების, სერვისის ფუნქციების, ენერგეტიკული პირობების, თავდასხმისგან დაუცველობისა და დროში ცვალებადი სხვა ატრიბუტების დიდი მრავალფეროვნების გამო. ვინაიდან თითოეულ სცენარს შეიძლება ჰქონდეს ენერგეტიკული უსაფრთხოებისა და ხელმისაწვდომობის უნიკალური მოთხოვნები, უსაფრთხოების სტრატეგიების შერჩევა და კონფიგურაცია უნდა იყოს ოპტიმიზებული 6G ქსელებისთვის ადაპტიური და დინამიკური გზით. **მეოთხე თავში** ვიკვლევთ 6G-ის უსაფრთხოებას გამომდინარე ენერგოეფექტიანობის პერსპექტივიდან, სხვადასხვა სცენარისთვის უსაფრთხოებისა და ენერგიის მოხმარების დაბალანსებით. კერძოდ, ჩვენ შევისწავლით AI-ზე მომუშავე 6G ქსელის არქიტექტურას პერსპექტიული აპლიკაციებითა და ხედვებით, შემდეგ განვსაზღვრავთ 6G-ში უსაფრთხოების ადაპტიური და დინამიკური ოპტიმიზაციის გამოწვე-

ვებს ჰეტეროგენულობის, დინამიკის და მოდელირების სირთულის თვალსაზრისით. უსაფრთხოებასა და ენერგეტიკას შორის კომპრომისის მისაღწევად, ჩვენ წარმოვადგენთ ოპტიმიზაციის სტრუქტურას, რომელიც უზრუნველყოფს უსაფრთხოების სტრატეგიის მორგებულ რეკომენდაციებს მომხმარებლის სხვადასხვა მოწყობილობისა და საბაზო სადგურებისთვის. ბოლოს განიხილება ღია საკითხები 6G უსაფრთხოების შესახებ ენერგოეფექტიანობის თვალსაზრისით.

6G-სთვის გათვალისწინებული ერთ-ერთი მნიშვნელოვანი მახასიათებელია უსაფრთხოების ფუნქციის ვირტუალიზაცია (SFV). 5G/B5G ქსელებში ქსელის ფუნქციის ვირტუალიზაციის (NFV) მსგავსად, SFV იძლევა ახალ შესაძლებლობებს უსაფრთხოების გასაუმჯობესებლად და ამავე დროს, უსაფრთხოების ოვერჰედის (სასიგნალო ხარჯების) შესამცირებლად. კერძოდ, ის უზრუნველყოფს უსაფრთხოებასთან დაკავშირებული თავსებადობის საკითხების გადაჭრის მიმზიდველ გზას. მავნე პროგრამული უზრუნველყოფით (malware) მავნე პროგრამების შეტანა საგნების ინტერნეტის (IoT) სისტემებში კიბერკრიმინალებს შორის პოპულარობას იძენს, 6G ქსელებში IoT მოწყობილობების რაოდენობის მოსალოდნელი ზრდის გამო. საუბარია SW-ზე, რომელიც სპეციალურად არის შექმნილი კომპიუტერულ სისტემაში შეფერხების, დაზიანების ან არასანქცირებული წვდომის მოსაპოვებლად. ამ პრობლემის გადასაჭრელად, **მეხუთე თავში** განხილულია უსაფრთხოების სტრუქტურა, რომელიც იყენებს უსაფრთხოების ფუნქციების SW-ის შემუშავებას SFV-ის საშუალებით, რათა გააუმჯობესოს სანდოობა IoT სისტემების მიმართ და შეძლებისდაგვარად თავიდან აიცილოს მავნე პროგრამის გავრცელება. IoT მოწყობილობები იყოფა სანდო, დაუცველ და კომპრომეტირებულ დონეებად დისტანციური ატესტაციის გამოყენებით. მოწყობილობების სამ განსხვავებულ კატეგორიაში იზოლირებისთვის, NFV გამოიყენება თითოეული კატეგორიისთვის ცალკეული ქსელის შესაქმნელად, ხოლო განაწილებული ლეჯერი გამოიყენება თითოეული მოწყობილობის მდგომარეობის შესანახად. ვირტუალიზებული დისტანციური ატესტაციის პროცედურები გამოიყენება ჰეტეროგენულ IoT მოწყობილობებს შორის თავსებადობის პრობლემების მოსაგვარებლად და მავნე პროგრამის გავრცელების ეფექტიანად თავიდან ასაცილებლად. შედეგები აჩვენებს, რომ შემოთავაზებულ სტრუქტურას შეუძლია ინფიცირებული მოწყობილობების რაოდენობა 66 პროცენტით შეამციროს მხოლოდ 10 წამის განმავლობაში.

მოსალოდნელია, რომ 6G შემოიტანს ქსელის ტექნოლოგიებს მაღალი გამტარუნარიანობით, მასობრივი კავშირებით და ფართო დაფარვით, რაც უზრუნველყოფს საგნების ინდუსტრიულ ინტერნეტს (IIoT), რომელიც მოითხოვს ულტრა დაბალ შეყოვნებას და ულტრა მაღალ საიმედოობას. IIoT არის ფიზიკური საინფორმაციო სისტემა, რომელიც შემუშავებულია ტრადიციულ ინდუსტრიული მართვის ქსელებზე დაყრდნობით და მოიცავს ინტელექტუალურ სატრანსპორტო სისტემებს, ჭკვიან ქარხნებს. როგორც ერთ-ერთი ყველაზე კრიტიკული ინფრასტრუქტურის სისტემა, IIoT ასევე სასურველი სამიზნეა მოწინავე მუდმივი საფრთხეების (APT) შემქმნელი თავდამსხმელებისათვის. ამ პრობლემის გადასაჭრელად, **მეექვსე თავში** გამოკვლეულია ღრმა სწავლებაზე (DL) დაფუძნებული APT-ის პროაქტიული გამოვლენის სქემა IIoT-ში. ამ სქემაში, თავდასხმების ხანგრძლივი მიმდევრობისა და გრძელვადიანი უწყვეტი APT თავდასხმის მახასიათებლების გათვალისწინებით, შემუშავებული მეთოდი იყენებს DL-ის ცნობილ მოდელს, ორმხრივი კოდერის წარმოდგენებს ტრანსფორმერებისგან (BERT), რათა გამოავლინოს APT თავდასხმების მიმდევრობები. ეს უკანასკნელი ასევე ოპტიმიზებულია მოდელის გრძელვადიანი მიმდევრობის შეფასების ეფექტიანობის უზრუნველსაყოფად. ექსპერიმენტული შედეგები არა მხოლოდ აჩვენებს, რომ შემოთავაზებულ DL მეთოდს აქვს მიზანშეწონილობა და ეფექტიანობა APT-ის გამოვლენისთვის, არამედ ადასტურებს, რომ BERT მოდელს აქვს უკეთესი სიზუსტე და ცრუ განგაშის დაბალი მაჩვენებელი APT თავდასხმების მიმდევრობის გამოვლენისას, ვიდრე სხვა დროითი მწკრივების მოდელებს.

6G უსადენო საკომუნიკაციო ქსელები მიზნად ისახავს საგნების ინდუსტრიული ინტერნეტის საშუალებით რევოლუცია მოახდინოს მომხმარებელთა სერვისებსა და აპლიკაციებში სრულად ინტელექტუალური, ავტონომიური სისტემების დანერგვით. ბოლოდროინდელი კვლევები გვიჩვენებს, რომ IIoT (განხილული წინა თავში) მნიშვნელოვან როლს შეასრულებს ტექნოლოგიური ინოვაციებისა და ინდუსტრიის კონკურენციის ახალ რაუნდში, რომლის მთავარი კომპონენტია იდენტურობის გარჩევადობის სისტემა. თუმცა, არსებობს გარკვეული პრობლემები ჰენდლზე (handle) დაფუძნებული იდენტურობის გარჩევადობის არქიტექტურაში. ამიტომ, ლიტერატურაში შემოთავაზებულია სანდო იდენტიფიკატორით ერთობლივი მმართველობის არქიტექტურა, ასევე შექმნილი და დანერგილია პროტოტიპის სისტემა, რაც განხილულია **მეშვიდე თავში.** კონკრეტულად, შემუშავებულია ბლოკჩეინზე დაფუძნებული დეცენტრალიზებული სტრუქტურა საიდენტიფიკაციო სერვისისთვის, იდენტიფიკატორის სასიცოცხლო ციკლის მართვა ჭკვიანი კონტრაქტის საფუძველზე და მონაცემთა შენახვის მექანიზმი სანდო იდენტიფიკატორისთვის. მთელ ამ არქიტექტურას შეუძლია გადაჭრას მტყუნების ერთი წერტილის, მონაცემთა გაყალბებისა და მმართველობის პროცესში გადახრების პრობლემები და შეამციროს მონაცემთა მიმოქცევის პროცესში სანდოობის ღირებულება. კომპიუტერული სიმულაციის შედეგები ცხადყოფს, რომ ამ სისტემას შეუძლია მიაღწიოს კარგ შედეგებს შეყოვნებისა და გამტარუნარიანობის თვალსაზრისით.

ვინაიდან 5G-ის კვლევა პრაქტიკულად დასრულებულია, კვლევითმა საზოგადოებამ უნდა გაიხედოს მის მიღმა და იმუშაოს 2030 წლისთვის დაკავშირების სხვადასხვა ვარიანტზე. ამ კონტექსტში, **მერვე თავი** განიხილავს წინსვლას 6G-ის ხედვისკენ შემდეგი თაობის საკომუნიკაციო პლატფორმის შეთავაზებით, რომელიც მიზნად ისახავს გააფართოოს ფიქსირებული განლაგების ქსელების ხისტი დაფარვის არეალი ვირტუალური მობილური პატარა ფიჭების (MSC) გათვალისწინებით, რომლებიც იქმნება შესაბამისი მოთხოვნების გათვალისწინებით. ახალი გამოთვლითი პარადიგმების საფუძველზე, როგორიცაა ქსელის ფუნქციების ვირტუალიზაცია და SW-ით განსაზღვრული ქსელი, ამ ფიჭებს შეუძლიათ გამოიყენონ რადიო და ქსელური შესაძლებლობები, ადგილობრივად შეამცირონ პროტოკოლის სიგნალის შეყოვნება და ოვერჰედი. ეს MSC-ები ქმნიან ქსელური რესურსების ინტელექტუალურ აუზს და მათ შეუძლიათ ერთობლივად შექმნან უსადენო MSC ქსელი, რომელიც უზრუნველყოფს საკომუნიკაციო პლატფორმას ლოკალიზებული, საყოველადგილო და საიმედო კავშირისთვის. აქ MSC კონცეფციის განხორციელების ტექნოლოგიური საშუალებები ასევე განიხილება ვირტუალიზაციის, უსადენო ქსელის „მსუბუქი“ უსაფრთხოებისა და ენერგოეფექტიანი რადიოსიხშირეების კუთხით. MSC არქიტექტურის უპირატესობები ფიჭების საიმედო და ეფექტიანი განტვირთვისათვის, ნაჩვენებია, როგორც გამოყენების შემთხვევა.

ინტეგრირებული ზონდირება და კომუნიკაცია (ISAC) ახლახან გამოჩნდა, როგორც 6G ტექნოლოგიის კანდიდატი, რომელიც მიზნად ისახავს მომავალი ქსელის ორი ძირითადი ოპერაციის გაერთიანებას სპექტრის, ენერგეტიკისა და დანახარჯების ეფექტიანად გამოყენების გზით. ISAC სისტემები ურთიერთობენ და გამოავლენენ სამიზნეებს საერთო ტალღის ფორმის, საერთო ტექნოლოგიური პლატფორმის და საბოლოოდ, იგივე ქსელის ინფრასტრუქტურის მეშვეობით. თუმცა, ინფორმაციული სიგნალის ჩართვა ზონდირების სიგნალის სახით სამიზნის აღმოჩენის მიზნით, ქმნის პრობლემებს ინფორმაციული უსაფრთხოების თვალსაზრისით. ამავდროულად, ISAC-ის გადაცემაში ინტეგრირებული გამოვლენის შესაძლებლობა გვთავაზობს უნიკალურ შესაძლებლობებს უსაფრთხო ISAC ტექნიკის შესაქმნელად. **მეცხრე თავი** განიხილავს ამ უნიკალურ გამოწვევებს და შესაძლებლობებს ISAC-ის შემდეგი თაობის ქსელებისთვის. ჩვენ ჯერ მოკლედ განვიხილავთ ტალღის ფორმის დიზაინის საფუძვლებს ზონდირებისა და კომუნიკაციისთვის, შემდეგ დეტალურად შევისწავლით ISAC-ის გადაცემის უსაფრთხოებასთან

დაკავშირებულ საკითხებს და წინააღმდეგობრივ მიზნებს, ასევე უსაფრთხოების მიმდინარე მიდგომებს; შემდეგ განვსაზღვრავთ ზონდირების შესაძლებლობების გამოყენების ახალ მეთოდიკას ცოდნის შესახებ მიზნობრივი ინფორმაციის მისაღებად, რომელიც ეფექტიანი მიდგომაა ფიზიკური ფენის უსაფრთხოების ცნობილი სისუსტეების წინააღმდეგ. დაბოლოს, ჩვენ ვაჩვენებთ რამდენიმე დაბალი ფასის მქონე უსაფრთხო ISAC არქიტექტურას, რასაც მოჰყვება კვლევებისთვის ღია თემების სერია. უსაფრთხო ISAC ტექნოლოგიების ეს ოჯახი უზრუნველყოფს ინფორმაციული უსაფრთხოების ახალ პერსპექტივას, ფოკუსირებულია საიმედო კონსტრუქციებზე შეზღუდული აპარატურული უზრუნველყოფით (HW) და მორგებულია იაფფასიან ISAC მოწყობილობებზე.

ერთ-ერთი ყველაზე პერსპექტიული და მაღალი პოტენციალის მქონე ტექნოლოგია, რომელიც მომავალი თაობის ქსელებში რადიოსიხშირული სპექტრის ეფექტიანად გამოყენების შესაძლებლობას იძლევა, ეს არის მოწყობილობებს შორის (D2D) კომუნიკაცია. დღეისათვის სამეცნიერო ლიტერატურაში ფართოდ განიხილავენ D2D კომუნიკაციის ორ ფუნდამენტურ და ურთიერთდაკავშირებულ ასპექტს, უსაფრთხოებას და კონფიდენციალურობას, რომლებიც აუცილებელია D2D-ის პრაქტიკული რეალიზაციისთვის. მიგვაჩნია, რომ ამ წიგნში წარმოდგენილი მეთოდები და ტექნოლოგიები შეიძლება წარმატებით იქნეს გამოყენებული 6G D2D კომუნიკაციებში მათი უსაფრთხოების გაუმჯობესებისთვის.

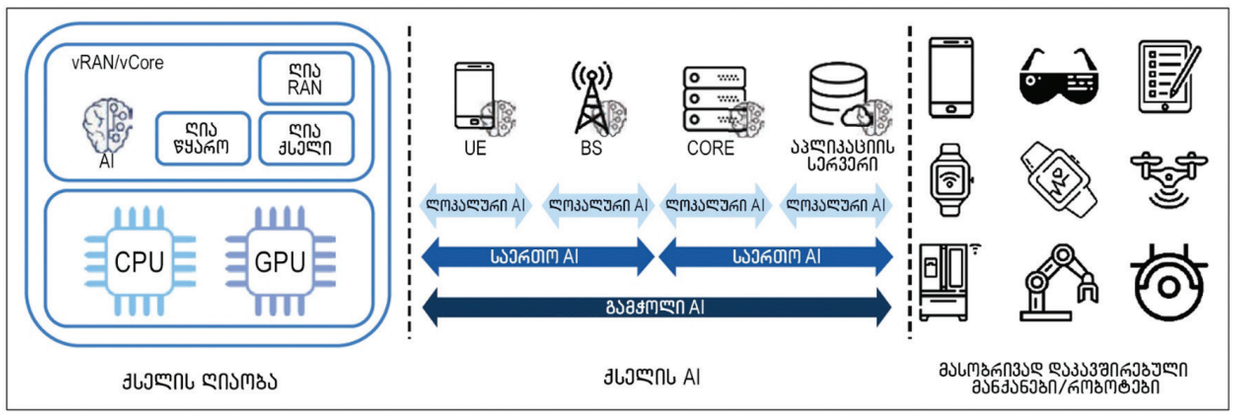
დამატებით აღვნიშნავთ, რომ წიგნის ბოლოს წარმოდგენილია გამოყენებული ინგლისურენოვანი აბრევიატურების და აკრონიმების მნიშვნელობები და მათი შესატყვისი ქართული თარგმანები.

ვფიქრობთ, მასალა სასარგებლო იქნება და დახმარებას გაუწევს საინფორმაციო ტექნოლოგიებისა და კომუნიკაციების დარგში მომუშავე სპეციალისტებს, აკადემიურ პერსონალს, ბაკალავრიატის მაღალი კურსის სტუდენტებს, მაგისტრანტებსა და დოქტორანტებს.

თავი 1. 6G ქსელების უსაფრთხოებასთან დაკავშირებული ტექნოლოგიური ტენდენციები და გადაწყვეტილებები

1.1. შესავალი

მიუხედავად იმისა, რომ ჩვენ დღეს 5G კომერციალიზაციის დაწყების მოწმენი ვართ, დროა დავიწყოთ მზადება 6G-სთვის, რომელიც ჩვენი ცხოვრების ნაწილი გახდება 2030 წელს და მის შემდგომ პერიოდში. უკვე მიმდინარეობს დისკუსიები 6G კომუნიკაციების მიმართულებებზე, რომელებსაც უძღვებიან აკადემიური წრეები, მოწყობილობების/აღჭურვილობის მომწოდებლები და ოპერატორები. 6G ტექნოლოგიების განვითარების მიმართულება გვიჩვენებს შემდეგ მეგატენდენციებს 6G-ის მიმართ: ქსელის ღიაობა (გახსნილობა), ქსელის ხელოვნური ინტელექტი (AI-ის გამოყენების გაფართოება) და მასობრივად დაკავშირებული მანქანები/რობოტები, როგორც ეს ნაჩვენებია ნახ. 1.1-ზე. პოტენციური ძირითადი სერვისები მოიცავს ჭეშმარიტად იმერსიულ გაფართოებულ რეალობას (XR), მაღალი სიზუსტის მობილურ ჰოლოგრამას, ციფრულ რეპლიკას, უპილოტო მანქანებსა და ტაქტილურ ინტერნეტს.



ნახ. 1.1. 6G-ის ძირითადი ტენდენციები

ტექნიკურ მახასიათებლებზე ჩვეულებრივი მოთხოვნების გარდა, როგორიცაა მონაცემთა გადაცემის სიჩქარე და შეყოვნება, რომლებიც განხილული იყო წინა თაობებში, სავარაუდოდ, სანდოობა იქნება 6G-ის აუცილებელი მოთხოვნა და ჩვენ უნდა განვავითაროთ 6G, როგორც ყველაზე უსაფრთხო მობილური საკომუნიკაციო ტექნოლოგია აქამდე არსებულებთან შედარებით. ტექნოლოგიური ტენდენციები, რომლებიც პირდაპირ გავლენას ახდენს უსაფრთხოებასა და კონფიდენციალურობაზე, მოიცავს ქსელის ღიაობას, SW-ზე დაფუძნებულ მობილურ საკომუნიკაციო სისტემებს, ვირტუალიზაციას/კონტეინერიზაციას, ქსელის AI-ის და კვანტურ გამოთვლებს.

6G-ისკენ მიმავალ გზაზე ძირითადი ტექნოლოგიური ტენდენციებია:

ქსელის ღიაობა და ღია წყაროს SW-ზე დაფუძნებული მობილური საკომუნიკაციო სისტემები: ვინაიდან ზოგადი დანიშნულების პროცესორების (როგორიცაა ცენტრალური პროცესორი (CPU) და გრაფიკული დამუშავების ბლოკი (GPU)) გამოთვლითი მახასიათებლები მნიშვნელოვნად უმჯობესდება, ქსელის ერთეულების (NE) დანერგვა, რომლებიც დაფუძნებულია ღია წყაროს SW-ზე სულ უფრო მიზანშეწონილი ხდება. ამ ტენდენციას შეუძლია შეამციროს ბარიერები ბაზარზე შესვლისთვის, ხელი შეუწყოს თავსებადობას და დააჩქაროს განვითარების ციკლი. შესაბამისი ინდუსტრიული საქმიანობის

მაგალითები მოიცავს ღია რადიოწვდომის ქსელის (ORAN) ალიანსს RAN-სთვის, ღია არქიტექტურითა და ინტერფეისით, და ღია ქსელის ავტომატიზაციის პლატფორმას (ONAP) ქსელის მართვისთვის და მისი ავტომატიზაციისთვის, ღია წყაროს შემცველი საერთო არქიტექტურის მეშვეობით.

ღია არქიტექტურაში თავდამსხმელს შეუძლია სცადოს შიდა სისტემებზე წვდომა ღია ინტერფეისის საშუალებით მოიპოვოს. თუ ავთენტიფიკაცია, ავტორიზაცია, წვდომის კონტროლი და კრიპტოგრაფიის ფუნქცია ადეკვატურად არ არის უზრუნველყოფილი ინტერფეისებში, თავდამსხმელი შეძლებს შეაღწიოს სისტემის შიგნით. გარდა ამისა, იმის გამო, რომ კოდები ერთობლივად არის შემუშავებული მრავალი დეველოპერის მიერ, შიდა ფუნქციები შეიძლება კონფლიქტში შევიდეს ერთმანეთთან. თავდამსხმელს შეუძლია გამოიყენოს ფუნქციების ასეთი კონფლიქტი, რათა სისტემაში მტყუნებები გამოიწვიოს.

ჰაკერებისთვის მარტივია სამიზნეების შერჩევა და დაუცველობის გაანალიზება ღია წყაროში, რადგან ღია წყაროს კოდები საჯაროდ ხელმისაწვდომია. ამიტომ, თუ ღია წყაროში დაუცველობა სწორად არ არის მართული, თავდამსხმელმა შეიძლება იგი სისტემაზე თავდასხმისთვის გამოიყენოს.

მომხმარებლის პერსონალური ინფორმაციის გამოყენება: კიდევ ერთი საყურადღებო ტენდენციაა პერსონალური, მაგრამ შესაძლოა ანონიმური მომხმარებლის ინფორმაციის გამოყენება მობილური ქსელის ოპერატორების (MNO) მიერ მოწოდებული სერვისების პერსონალიზებული სერვისის ხარისხის (QoS) და გამოცდილების ხარისხის (QoE) გასაუმჯობესებლად. თუმცა, მომხმარებლის ინფორმაციაზე გარე წვდომის ინტერფეისები წარმოქმნიან თავდასხმის ზედაპირს მომხმარებლის ინფორმაციის გაჟონვისთვის. გარდა ამისა, სუსტი უსაფრთხოების მქონე დაკავშირებული აპარატის გატეხვა შესაძლებელია მოწყობილობის პერსონალურ მონაცემებზე და აბონენტის ინფორმაციაზე წვდომის მოსაპოვებლად.

ქსელის AI: სავარაუდოდ, AI გახდება 6G სისტემის ძირითადი შემადგენელი კომპონენტი. NE დაამუშავებს დიდი რაოდენობით მონაცემს და AI-ის ძალისხმევით მოახდენს ქსელის მუშაობის ოპტიმიზაციას რეალურ დროში. მოსალოდნელია, რომ ეს განხორციელდება AI-ის გამოყენებით ტექნოლოგიური დიზაინის ეტაპიდან და ადგილობრივი AI-ის, ერთობლივი AI-ის და გამჭოლი (ბოლოების დამაკავშირებელი) AI-ის ფუნქციების ინტერნალიზებით. ადგილობრივი AI, დანერგილი თითოეულ NE-ში, შეიძლება გამოყენებულ იქნეს მოდულაციის, წყაროს კოდირებისა და არხის კოდირების ოპტიმიზაციისთვის. ერთობლივ AI-ის შეუძლია NE-ებს შორის თანამშრომლობის ოპტიმიზაცია. ერთობლივი AI-ის მაგალითია ჰენდოვერის (HO) ოპტიმიზაცია, რომელიც ეფუძნება მომავალი ქსელის პირობების პროგნოზირებას რთულ უსადენო გარემოში. გამჭოლი AI ნიშნავს ქსელის საერთო მუშაობის ოპტიმიზაციას ქსელში გენერირებული ინფორმაციის ანალიზით. გამჭოლი AI-ის მაგალითებია QoS-ის ოპტიმიზაცია, ფიჭის ჩართვა/გამორთვა ენერგიის მოხმარების მინიმიზაციისთვის, თვალთვალის არეალის და რეგისტრაციის არეალის ოპტიმიზაცია სიგნალის ოვერჰედის შემცირებისთვის.

თუმცა, AI ზოგჯერ არასწორად ახდენს მონაცემების კლასიფიკაციას, რომლებიც ოდნავ განსხვავდება მონაცემთა განაწილებიდან მიღებული, სწორად კლასიფიცირებული მონაცემებისგან. არასწორი კლასიფიკაციის მახასიათებლების გამოყენებით, თავდამსხმელს შეუძლია მოატყუოს AI-ის მოდელი არასწორი და შეცდომაში შემყვანი მონაცემების მიწოდებით, რომლებიც განზრახ შეცვლილია ქსელის სისტემის არასტაბილურობის, გაუმართაობის ან მიუწვდომელობის მისაღწევად, რასაც AML ეწოდება.

ვირტუალიზაცია და კონტეინერიზაცია: ვირტუალიზაცია არის ტექნოლოგია, რომელიც საშუალებას აძლევს ერთი ფიზიკური მოწყობილობის HW-ის რესურსს დაიყოს მრავალ ლოგიკურ HW რესურსად, რომელსაც ეწოდება ვირტუალური მანქანები (VM), და VM მუშაობს ლოგიკურ HW რესურსზე.

ჰიპერვიზორი არის ტიპური SW, რომელიც ვირტუალიზაციის საშუალებას იძლევა. ამრიგად, ჰიპერვიზორს შეუძლია მოახდინოს VM-ების რესურსების მონიტორინგი და მხარი დაუჭიროს თითოეულ VM-ის საიმედო იზოლაციას სხვებისგან. კონტეინერიზაცია არის პაკეტის აპლიკაციების კონცეფცია ასოცირებულ ბიბლიოთეკებთან და დამოკიდებულებებთან, რაც ქმნის იზოლირებულ გარემოს ოპერაციული სისტემის (OS) დონეზე პროგრამული სერვისების გასაშვებად. ვირტუალიზაციასთან შედარებით, კონტეინერები ერთობლივად იყენებენ OS-ის ბირთვს, უფრო სწრაფად მოდიან მოქმედებაში და ნაკლებ მეხსიერებას იკავებენ.

ვირტუალიზაციის/კონტეინერიზაციის გამოყენებით ოპერატორებს აქვთ დიდი უპირატესობა კაპიტალური დანახარჯების (CAPEX) და საოპერაციო დანახარჯების (OPEX) თვალსაზრისით. CAPEX-ის ეფექტიანობის მიღწევა შესაძლებელია მხოლოდ ვირტუალური RAN-სთვის და ვირტუალური ძირითადი ქსელისთვის (Core), ანუ vRAN/vCore-სთვის საჭირო რესურსების გამოყოფით. გარდა ამისა, VM-ები/კონტეინერები, რომლებიც დროებით შეჩერებულია ან საერთოდ გაჩერებულია, შეიძლება დაუყოვნებლივ გადაიტვირთოს დროებით შეჩერებული ან გაჩერებული მდგომარეობიდან. თუ მრავალი მომხმარებლის მოწყობილობა (UE) აქტიურად არის დაკავშირებული კონკრეტულ vRAN-თან, მაგალითად, ქალაქის ცენტრში მოწყობილი დღესასწაულისას ან სტადიონზე დიდი სპორტული ღონისძიების დროს, vRAN შეიძლება ადვილად იქნეს გადატანილი HW-ზე მაღალი გამოთვლითი სიმძლავრით, სერვისის შეფერხების გარეშე, პირდაპირი მიგრაციის საშუალებით. ამრიგად, ოპერატორებს შეუძლიათ მიაღწიონ OPEX-ის ეფექტიანობას.

წინა თაობების შემუშავების პროცესში (მათ შორის, 5G-ის) ვირტუალიზაცია და კონტეინერიზაცია არ იყო გათვალისწინებული უსაფრთხოების ასპექტებში. ვირტუალიზაციის ფენა და მასპინძელი (host) OS გახდა ახალი დაუცველობებით და თავდასხმის ვექტორებით გამოწვეული დიდი გამოწვევა უსაფრთხოებისთვის.

კვანტური გამოთვლები: კვანტურ გამოთვლებს (QC) შეუძლია სწრაფად გადაჭრას ისეთი რთული გამოთვლითი პრობლემები, როგორიცაა: ძალიან დიდი რიცხვის მარტივი ფაქტორიზაცია და დისკრეტული ლოგარითმების პრობლემა კვანტური მექანიკური თვისებების გამოყენებით, სუპერპოზიცია და კვანტური ჩახლართულობა (quantum entanglement). სავარაუდოდ, QC ფართოდ ხელმისაწვდომი იქნება 6G-ის ეპოქაში. შესაბამისად, 6G-ის დანერგვის პროცესში აუცილებელია მომზადება QC-ის წარმოქმნით გამოწვეული ზემოქმედებისთვის. მაგალითად, QC-ის რეალიზაცია სავარაუდოდ, გავლენას მოახდენს არსებული კრიპტოგრაფიული ალგორითმების უსაფრთხოებაზე, რომლებიც თანამედროვე მობილურ ქსელებში გამოიყენება.

პირველი თავის დანარჩენი ნაწილი შემდეგნაირად არის ორგანიზებული: ჩვენ ჯერ ვიკვლევთ უსაფრთხოების მიმართ კონკრეტულ საფრთხეებს ზემოაღნიშნული ტექნოლოგიური ტენდენციებიდან გამომდინარე, რის შემდეგაც განვიხილავთ შესაძლო გადაწყვეტილებებს ამ საფრთხეების შესამცირებლად, თავის ბოლოს კი წარმოვადგენთ შესაბამის დასკვნებს.

1.2. ტექნოლოგიური ტენდენციებიდან გამომდინარე 6G-ის წინაშე მდგარი უსაფრთხოების პრობლემები

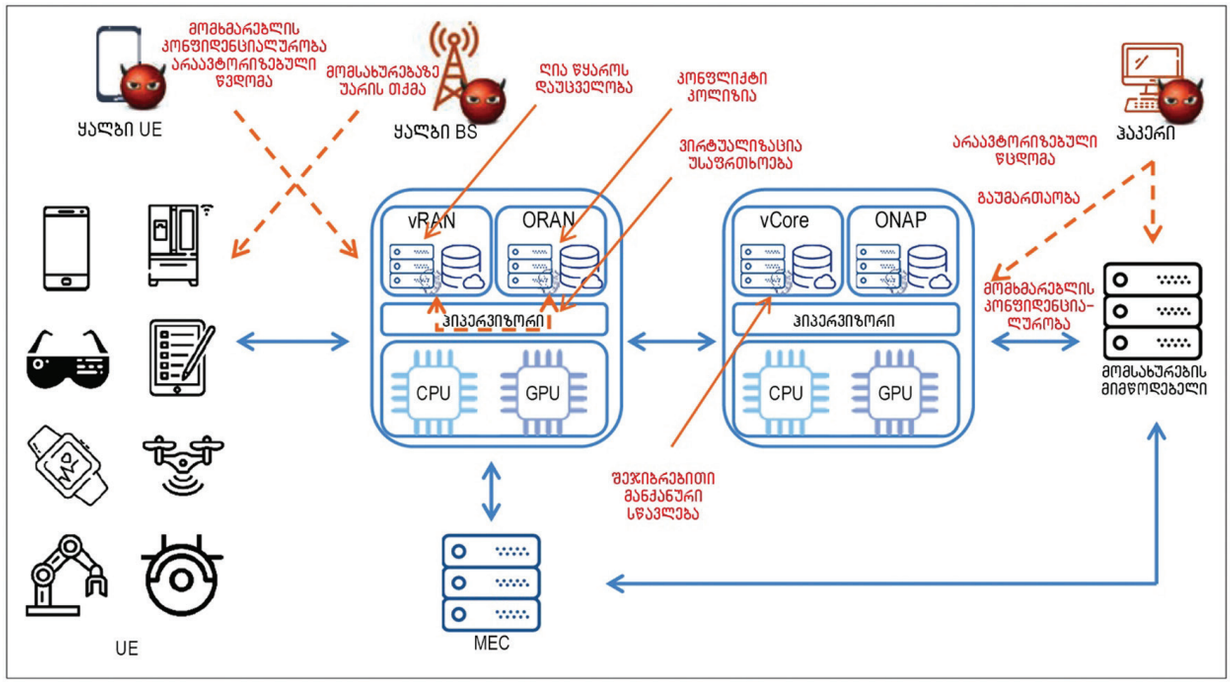
ამ პარაგრაფში 6G-ის მიმართულებით ძირითადი ტექნოლოგიური ტენდენციები შეჯამებულია ხუთ ძირითად კატეგორიად და განხილულია უსაფრთხოების პრობლემები, რომლებიც დაკავშირებულია თითოეულ ტექნოლოგიურ ტენდენციასთან. ნახ. 1.2 წარმოგვიდგენს უსაფრთხოების პრობლემებს 6G ქსელში და თითოეული კონკრეტული საფრთხე ჩამოთვლილია ცხრილში 1.1.

1.2.1. ღიაობით გამოწვეული საფრთხეები

ქსელის ღიაობა დიდწილად, ორ კატეგორიად იყოფა: გამომდინარე არქიტექტურული პერსპექტივიდან და მიღებული ღია წყაროს გამოყენების შედეგად.

საფრთხეები ღია ქსელის არქიტექტურიდან SW-ზე დაფუძნებული მობილური საკომუნიკაციო სისტემისთვის: არსებულ მობილურ საკომუნიკაციო სისტემებში, გარეთ განთავსებულ NE-ებს შეუძლიათ შიგნით წვდომა საზღვარზე საიდუმლო უფლებამოსილების გამოყენებით, როგორიცაა 5G ავთენტიფიკაცია და გასაღებების შესახებ შეთანხმება (AKA), ინტერნეტპროტოკოლის უსაფრთხოება (IPSec) და გაფართოებადი ავთენტიფიკაციის პროტოკოლ-ტრანსპორტის ფენის უსაფრთხოება (EAP-TLS), რომელიც დაფუძნებულია პერიმეტრის უსაფრთხოების არქიტექტურაზე. ამრიგად, სისტემის უსაფრთხოება დამოკიდებულია ქსელის ობიექტისა და ინტერფეისის უსაფრთხოებაზე. როდესაც არსებობს მრავალი NE და ინტერფეისი, სისტემის უსაფრთხოება კონვერგირდება ყველაზე სუსტი წერტილის უსაფრთხოებამდე. როდესაც თავდასხმის ზედაპირების რაოდენობა იზრდება, თავდამსხმელს სუსტი წერტილების პოვნის მეტი შესაძლებლობა აქვს.

იმის გამო, რომ დაკავშირებული მოწყობილობების რაოდენობა სავარაუდოდ, 2030 წლისთვის 500 მილიარდ მოწყობილობას მიაღწევს, თავდასხმის ზედაპირი სწრაფად გაიზრდება. კერძოდ, მოსალოდნელია, რომ დაკავშირებულ მანქანებს უსაფრთხოების შედარებით დაბალი მაჩვენებლებით, როგორიცაა: დრონები, საყოფაცხოვრებო ტექნიკა და ჭკვიანი სენსორები, შეეძლებათ 6G მობილური კომუნიკაციის სისტემებზე წვდომა. შესაბამისად, ეს სისტემები შეიძლება გახდეს უფრო დაუცველი ისეთ გარემოში, სადაც ცუდი უსაფრთხოების მქონე მოწყობილობებს აქვთ წვდომა მობილურ საკომუნიკაციო სისტემებთან.



ნახ. 1.2. საფრთხეების ლანდშაფტი 6G-ში

5G-ში, ქსელის ექსპოზიციის ფუნქცია (NEF), რომელიც შემოღებულია კონკრეტულ UE-ებთან დაკავშირებული სერვისების გარე ექსპოზიციისთვის, შიდა საკომუნიკაციო ტრაფიკზე ახდენს გავლენას. მობილურ პერიფერიულ გამოთვლებს (MEC), დანერგილს ულტრა დაბალი შეყოვნების სერვისისთვის,

ასევე აქვს UE/RAN/აპლიკაცია ინფორმაციაზე წვდომა. მესამე მხარეს შეუძლია სისტემაზე წვდომა NEF-ისა და MEC-ის მეშვეობით, რათა მათი გამოყენებითი სერვისების მახასიათებლებს ოპტიმიზაცია გაუწიოს და მორგებული სერვისი თითოეული აბონენტისთვის უზრუნველყოს. ანალოგიურად, 6G-ში მოსალოდნელია, რომ NEF/MEC და მასთან დაკავშირებული ინტერფეისები, შემდგომში გაიხსნება მესამე მხარეებისთვის 5G-სთან შედარებით, QoS/QoE-ის შემდგომ გასაუმჯობესებლად. ამიტომ, 6G-ში პერსონალიზებული ტექნოლოგიის ინტერფეისები ასევე აღებს კარს კონფიდენციალურობაში მცირემასშტაბიანი შეჭრისთვის.

მაგალითად, ORAN სისტემა მოიცავს დამატებით ფუნქციებს, როგორებიცაა: სერვისის მართვისა და ორკესტრირების სტრუქტურა, RAN-ის ინტელექტუალური კონტროლერი (RIC) არარეალურ დროში, ანუ NRT RIC და RIC თითქმის რეალურ დროში (nRT RIC) და იგი ახლებურად წარმოგვიდგენს ფრონტჰოლის ღია ინტერფეისებს, როგორებიცაა: A1, E2, O1, O2, ახლად განსაზღვრული ქსელის ფუნქციებთან (NF) კომუნიკაციისთვის. nRT RIC არის ლოგიკური AI ფუნქცია RAN-ში და მისი გამოყენება შესაძლებელია რადიორესურსების მართვისთვის (RRM) და რეალურ დროში ოპტიმიზაციისთვის. ORAN სისტემაში, ვინაიდან RRM მკაფიოდ არ არის გამიჯნული nRT RIC-სა და RAN-ს შორის, შეიძლება მოხდეს მმართველი სიგნალების კონფლიქტი. თუ თავდამსხმელი ასეთ კონფლიქტს გამოიყენებს, ამან შეიძლება გამოიწვიოს ქსელის არასტაბილურობა და „სერვისზე უარის თქმის“ (DoS) ტიპის თავდასხმა, რომელიც რადიორესურსებს ამოწურავს. გარდა ამისა, nRT RIC-ს შეუძლია მართოს კონკრეტული ფიჩის ან UE-ების ქცევა ქსელის მახასიათებლის ან მომხმარებელთან ურთიერთქმედების ოპტიმიზაციისთვის. ამიტომ, თავდამსხმელს შეუძლია სცადოს თავდასხმა nRT RIC-ზე, რათა გამოიწვიოს გაუმართაობა და მოიპოვოს პირადი ინფორმაცია კონკრეტული აბონენტის თვალთვალის გზით ან გამოიწვიოს სერვისის გათიშვა.

საფრთხეები ღია წყაროდან: ღია წყაროს თანდაყოლილი დაუცველობის რაოდენობა ყოველწლიურად იზრდება – 2008 წლის 500-დან 2019 წლის 6000-ზე მეტ დაუცველობამდე. გამოვლენილი დაუცველობები ინდექსირებულია აშშ-ის მთავრობის მიერ მხარდაჭერილი კოორპორაცია MITRE-ის მიერ და უზრუნველყოფს დაუცველობის დეტალურ ანალიზს. ვინაიდან წყაროს კოდი ღიაა, თავდამსხმელისთვის მარტივია თავდასხმის მეთოდის შერჩევა და სამიზნის მოქმედების ანალიზი. ღია წყაროები, რომლებიც არ არის კარგად მოვლილი, კიდევ უფრო დაუცველია, რადგან ან არასწორი პატჩებია (საკერებლები) მოწოდებული (პატჩი არის SW-ის პატარა „ნაჭერი“, რომელიც გამოიყენება პრობლემის გამოსასწორებლად), ან ხშირად, ისინი ცუდად არის გამოყენებული. გარდა ამისა, თუ დეველოპერი არ არის დაინტერესებული უსაფრთხოებით, არ ამოიცნობს პრობლემას და დაუყოვნებლივ არ გაასწორებს მას პატჩით, სისტემის წინაშე მდგარი საფრთხეები შეიძლება მნიშვნელოვნად გაიზარდოს. გარდა ამისა, დაუცველობის მონაცემთა ბაზის (DB) გამოყენებით, თავდამსხმელებს შეუძლიათ ადვილად შეიმუშაონ მეთოდები დაუცველობისთვის და ჰაკერული ინსტრუმენტებიც კი მიიღონ საჯარო ქსელებში ან დარქნეტში დაუცველობის გამოსაყენებლად, როგორიცაა kali linux ან metasploit. ღია წყაროში დაუცველობის გამოყენებისას, თავდამსხმელმა შეიძლება ადვილად გაამჟღავნოს მომხმარებლის მდებარეობა/პერსონალური ინფორმაცია, გამოიწვიოს მობილური საკომუნიკაციო სისტემის სერვისის DoS და ასევე, მობილური კომუნიკაციის გაუმართაობა.

1.2.2. შეჯიბრებითი მანქანური სწავლებით გამოწვეული საფრთხეები

ვინაიდან AML იყენებს AI-ის ალგორითმების თანდაყოლილ სისუსტეებს, AI-ის შემცველი მობილური საკომუნიკაციო სისტემები უფრო დაუცველი გახდება. მაგალითად, თავდამსხმელს შეუძლია პირადი ინფორმაციის ამოღება, AI მოდელის მიმართ „მოდელის ინვერსიით“ ტიპის თავდასხმის განხო-

რციელებით, რათა მოახდინოს მორგებული QoS ოპტიმიზაცია თითოეული მომხმარებლისთვის. მონაცემების მოწამვლაზე ორიენტირებული თავდასხმით, Microsoft-ის ჩატ-ბოტი Tay-ის მანიპულირებული ინფორმაციით, ტრენინგის საშუალებით, თავდამსხმელი იწვევს Tay-ის გაუმართაობას. ანალოგიურად, მავნე UE-მ შეიძლება მოახდინოს შეცდომაში შემყვანი ტრენინგის მონაცემების რეგულირება, რითაც გააუარესებს მთლიან მახასიათებლებს ან გამოიწვევს გაუმართაობას. მოდელიდან არიდების თავდასხმის გამოყენებისას, UE მანიპულირებულ შემავალ მონაცემებს გადასცემს ნორმალური სიგნალის სიმძლავრის გაზომვის ინფორმაციაზე სპეციფიკური ინფორმაციის დამატების გზით, რითაც ამცირებს HO-ის ან სხივის თვალყურის დევნების და მართვის ეფექტიანობას. გარდა ამისა, მოდელის მოპოვების თავდასხმის საშუალებით, ოპერატორების ან მიმწოდებლების AI მოდელი და ინტელექტუალური საკუთრება შეიძლება ამოღებული და გამოყენებული იქნეს ნებართვის გარეშე. თუ AI მოდელის კონფიდენციალურობა არ არის გარანტირებული, თავდამსხმელს შეუძლია გააანალიზოს AI მოდელი დაუცველობის აღმოსაჩენად და გამოიყენოს, როგორც საწყისი წერტილი შემდგომი თავდასხმებისთვის.

ტექნოლოგიური მიმართულებები	უსაფრთხოების წინაშე მდგარი საფრთხეები	გადაწყვეტილებები
ქსელის ღიაობა	არაავტორიზებული წვდომა და წვდომის შემოვლითი გზა	PKI და ნულოვანი სანდოობის არქიტექტურა
	დაბალი უსაფრთხოების მქონე მანქანები	უსაფრთხოების მართვის სისტემა
	არაავტორიზებული წვდომა ღია ინტერფეისში	იდენტიფიკაციის და ავთენტიფიკაციის მენეჯმენტი
	SW კონფლიქტები	კონფლიქტების მიგრაცია
SW-ზე დაფუძნებული მობილური საკომუნიკაციო სისტემა ღია წყაროთი	გამოუვლენელი დაუცველობა	დაუცველობის ავტომატიზებული მენეჯმენტის სისტემა
	ღია წყარო პატჩის დადების გარეშე	პატჩის ავტომატური სისტემა, უსაფრთხო OTA
ვირტუალიზაცია და კონტეინერიზაცია	კომპრომეტირებული ჰიპერვიზორი	აღსრულების სანდო გარემო
	პრივილეგიის ესკალაცია	ვირტუალიზაციის უსაფრთხო ფენა
	VM-შორისი თავდასხმა	ვირტუალური მანქანის თვითანალიზი
	დაუცველობის გავრცელება ცოცხალი მიგრაციით	უსაფრთხო ცოცხალი მიგრაცია
	არაავტორიზებული წვდომა, პაკეტების ანალიზი სოკეტზე	OS-დონეზე უსაფრთხო კონფიგურაცია
მომხმარებლის ინფორმაციის გამოყენება	არაავტორიზებული წვდომა	წყაროს ავთენტიფიკაცია და ავტორიზაცია
	არაავტორიზებული გამოყენება	მომხმარებლის ინფორმაციის გამოყენების უსაფრთხო პროცედურები
	მომხმარებლის ინფორმაციის ამოღება	აღსრულების სანდო გარემო
	თავდასხმები UE იდენტიფიკატორის ხელში ჩაგდებით	უსაფრთხო იდენტიფიკატორის მინიჭება
ქსელის AI	AI-ის გაუმართაობა	AI ინტერფეისის სანდო სისტემები
	თავდასხმა მოდელის ინვერსიით	AI ტრენინგი კონფედენციალურობის გაუმჯობესებული ტექნოლოგიებით
	თავდასხმა მონაცემების მოწამვლით	AI მონაცემების სანდო შეგროვება
	თავდასხმა მოდელიდან არიდებით	AI ოპერაციების სტატისტიკური ანალიზი
	თავდასხმა მოდელის მოპოვებით	ანომალიების გამოვლენა ზღურბლის მიხედვით
კვანტური გამოთვლების შემოტანა	დაუცველი ასიმეტრიული გასაღების ალგორითმი	პოსტკვანტური კრიპტოგრაფიის შემოტანა

ცხრილი 1.1. 6G უსაფრთხოება: სანდო გადაწყვეტილებები სხვადასხვა ტიპის საფრთხისთვის

1.2.3. კონფიდენციალურობის საფრთხეები

მოსალოდნელია, რომ MNO-ები და სერვისის გარე პროვაიდერები აანალიზებენ მომხმარებლის ინფორმაციას სხვადასხვა გზით მონაცემთა ანალიზისა და AI ტექნოლოგიების გამოყენებით. მაგალითად, მობილურობის ისტორია და სერვისის/აპლიკაციის გამოყენების ჟურნალი თითოეული მომხმარებლისთვის შეიძლება გაანალიზდეს QoS-ის და QoE-ის გასაუმჯობესებლად. ვინაიდან AI და მონაცემთა ანალიზი ფართოდ გამოიყენება სხვადასხვა სერვისში, მომხმარებლის ინფორმაციის გამოყენება მნიშვნელოვანი ხდება.

თუმცა, პერსონალიზაციის ტექნოლოგიები 6G-ში აღებს კარს კონფიდენციალურობის კუთხით მცირემასშტაბიანი შეჭრისთვის. საიმედო და უსაფრთხო გარემოს გარეშე, მომხმარებლის შესახებ ინფორმაციის გამოყენებამ შეიძლება ამ ინფორმაციის გაჟონვა გამოიწვიოს და შექმნას სერიოზული საფრთხე მომხმარებლის კონფიდენციალურობის დაცვის კუთხით. გარდა ამისა, თუ მობილური საკომუნიკაციო სისტემა სათანადოდ არ მართავს აბონენტის იდენტიფიკატორებს, როგორიცაა რადიოქსელის დროებითი იდენტიფიკატორი (RNTI) და გლობალურად უნიკალური დროებითი იდენტიფიკატორი (GUTI), თავდამსხმელს შეუძლია გაარკვიოს კონკრეტული მომხმარებლის მდებარეობა RNTI-ის და GUTI-ის თვალთვალის გზით. ლიტერატურაში ნაჩვენებია, რომ თავდამსხმელს შეუძლია შეიტყოს მომხმარებლის პერსონალური ინფორმაცია, როგორიცაა UE-ში შესრულებული აპლიკაციები და სერვისების ინფორმაცია, გრძელვადიანი ევოლუციის ანუ LTE-ის გადაცემული დაუნლინკის მმართველი ინფორმაციის შესაბამისი შეტყობინებების ანალიზით, ღრმა სწავლების გამოყენებით.

გარდა ამისა, პერსონალური ინფორმაციის დასაცავად სხვადასხვა ქვეყანა იღებს კანონებს. 2018 წელს ევროკავშირმა შემოიღო მონაცემთა დაცვის ზოგადი რეგლამენტი მონაცემთა სუბიექტების უფლებებისა და კორპორაციული ანგარიშვალდებულების გასაძლიერებლად. კალიფორნიის მომხმარებელთა კონფიდენციალურობის აქტი მიღებულია, ხოლო მომხმარებელთა ონლაინკონფიდენციალურობის უფლებების აქტი განხილვის პროცესშია ამერიკის შეერთებული შტატების ფედერალურ დონეზე. ჩინეთის სახალხო რესპუბლიკამ 2020 წელს მიიღო კანონი მონაცემთა კონფიდენციალურობის შესახებ, რომელიც განსაზღვრავს პერსონალური მონაცემების დაცვის პროცედურებსა და ვალდებულებებს. სამხრეთ კორეაში 2020 წელს ამოქმედდა სამი კანონი პერსონალური ინფორმაციის დაცვის შესახებ. კანონების დარღვევის შემთხვევაში, MNO-ებმა შეიძლება გადაიხადონ ჯარიმები, როგორც სასჯელი კონფიდენციალურობისთვის მიყენებული ზიანისთვის.

1.2.4. ვირტუალიზაციის/კონტეინერიზაციის საფრთხეები

ვირტუალიზაციის დანერგვა უსაფრთხოების კუთხით რამდენიმე ახალ პრობლემას ქმნის. ვინაიდან ჰიპერვიზორს შეუძლია VM-ების რესურსების მონიტორინგი, ის უსაფრთხო უნდა იყოს. თუ თავდამსხმელმა კონკრეტული ჰიპერვიზორის წინააღმდეგ დაფუძნება მოახერხა, მას შეეძლება მიიღოს ყველა პრივილეგია vRAN/vCore-ზე, რომელიც მუშაობს კომპრომეტირებულ ჰიპერვიზორზე და შესაბამისად, შეძლებს შეუტიოს მობილურ საკომუნიკაციო სისტემას.

გარდა ამისა, იმის გამო, რომ VM-ებს შორის კომუნიკაცია შიდა ვირტუალური გადამრთველის საშუალებით ხორციელდება, შეიძლება გაჩნდეს თავდასხმის ახალი გზა. თავდამსხმელი იჯარით იღებს რესურსებს იმავე HW-სთვის, როგორც vRAN/vCore და აყენებს მავნე VM-ს. თავდამსხმელი ასევე გატეხავს VM-ს იმავე HW-ზე, როგორც vRAN/vCore და იყენებს კომპრომეტირებულ VM-ს, როგორც შუალედურ წერტილს vRAN/vCore-ზე თავდასხმისთვის. შედეგად, შესაძლებლობა ექნებათ გამოიწვიონ ჩანერგვა,

DoS, პაკეტის ამოცნობა, მავნე კოდის გავრცელება და გვერდითი არხის თავდასხმები vRAN/vCore-ზე ვირტუალიზებულ სისტემაში. სამწუხაროდ, უსაფრთხოების ტრადიციული ტექნოლოგიები, როგორიცაა შეჭრის აღმოჩენის სისტემა (IDS), შეჭრის პრევენციის სისტემა (IPS) და ქსელის უსაფრთხოების მოწყობილობა – firewall, ვირტუალიზაციის სისტემის გარეთ არსებობს. შესაბამისად, ძნელია ვირტუალიზებულ სისტემაში შეჭრის აღმოჩენა, რითაც უსაფრთხოების ბრმა ზონა იქმნება.

ვინაიდან ვირტუალიზაცია აადვილებს VM-ების გადაადგილებას ფიზიკურ HW-ებს შორის, რაც ცოცხალ მიგრაციას წააგავს, vRAN/vCore-ში დაუცველობა შეიძლება ადვილად და სწრაფად გავრცელდეს მრავალ ფიზიკურ HW მოწყობილობაზე. თუ თავდამსხმელს შეუძლია რამდენიმე vRAN/vCore-დან ერთის გატეხვა, ის შეიძლება მუდმივად ეცადოს გამოიყენოს APT მობილური კომუნიკაციის სისტემაში.

კონტეინერიზაცია ეს არის ვირტუალიზაცია OS დონეზე. ამრიგად, მასპინძელი OS დაცული უნდა იყოს თავდამსხმელებისგან, რომლებიც პრივილეგიების გაფართოებას ცდილობენ. თუ მასპინძელი OS არ არის სწორად კონფიგურირებული, თავდამსხმელს შეუძლია თავდასხმა სხვა კონტეინერებზე, მავნე კონტეინერის გამოყენებით. მაგალითად, თუ მასპინძელი OS არ ამუშავებს რესურსებზე წვდომის პრივილეგიებს, თავდამსხმელს შეუძლია მასპინძელ OS რესურსებზე წვდომა სცადოს. გარდა ამისა, თუ მასპინძელი OS არ ახდენს კონტეინერების ქსელის იზოლირებას ქსელის სახელების სივრცის გამოყენებით, მავნე კონტეინერს შეუძლია სხვა კონტეინერების საკომუნიკაციო პაკეტების ანალიზი გადაცემის მართვის პროტოკოლის (TCP) სოკეტზე. კონტეინერების ცოცხალი მიგრაციის გამო, მათ შიგნით დაუცველობა ადვილად შეიძლება გავრცელდეს მრავალ OS-ზეც.

1.2.5. კვანტური გამოთვლების დანერგვით გამოწვეული საფრთხეები

ალგორითმები ასიმეტრიული გასაღებით გამოიყენება ავთენტიფიკაციის, წვდომის კონტროლის, კონფიდენციალურობის, მთლიანობისა და საიმედოობის მხარდასაჭერად მობილურ საკომუნიკაციო სისტემებში. კერძოდ, ალგორითმები ასიმეტრიული გასაღებით მიღებულია სხვადასხვა პროცედურაში. ხელმოწერის მუდმივი იდენტიფიკატორი დაშიფრულია ასიმეტრიული გასაღების ალგორითმით თავდაპირველი ავთენტიფიკაციის დროს, აბონენტების კონფიდენციალურობის უზრუნველყოფისთვის. პირველადი ავთენტიფიკაციის პროცესში, კერძო ქსელში დაინერგა სერტიფიკატზე დაფუძნებული EAP-TLS პროტოკოლი. სერტიფიკატი ციფრულად არის ხელმოწერილი ასიმეტრიული გასაღების ალგორითმის გამოყენებით.

NEF-სა და მესამე მხარის აპლიკაციის ფუნქციას შორის ინტერფეისში, სერტიფიკატზე დაფუძნებული TLS და ღია ავტორიზაცია ასევე გამოიყენება აპლიკაციის პროგრამირების საერთო ინტერფეისის სტრუქტურაში (CAPIF), რომელიც არის მე-3 თაობის პარტნიორობის პროექტი (3GPP) Northbound API. პერიფერიული უსაფრთხოების დაცვის პროქსი-სერვერი (SEPP) დანერგილია კომუნიკაციის მხარდასაჭერად NF-ებს შორის, რომლებიც სხვადასხვა მობილურ ქსელს მიეკუთვნებიან. SEPP იყენებს JSON ვებ-დაშიფვრას შეტყობინებების დასაცავად, ხოლო ინტერნეტპროტოკოლის (IP) გაცვლის სერვისის პროვაიდერი იყენებს JSON ვებ-ხელმოწერას სერვისზე დაფუძნებულ არქიტექტურაში.

არსებული მობილური საკომუნიკაციო სისტემების ზემოაღნიშნულ პროცედურებში ასიმეტრიული ალგორითმების უსაფრთხოება დიდი რიცხვის მარტივ რიცხვებად ფაქტორიზაციის პრობლემის სირთულესა და დისკრეტული ლოგარითმების პრობლემას ეფუძნება. თუმცა, ვინაიდან QC-ის შეუძლია პრობლემების სწრაფად გადაჭრა, ზემოაღნიშნული უსაფრთხოების პროცედურები აღარ არის უსაფრთხო მას შემდეგ, რაც QC ხელმისაწვდომი გახდება.

1.3. გზა 6G-ის უსაფრთხოების მიმართულებით: გადაწყვეტილებები სანდოობისთვის

უსაფრთხოების წინაშე მდგარი საფრთხეების მზარდი რისკის გათვალისწინებით, ჩვენ ველით, რომ სანდოობა გახდება აუცილებელი მოთხოვნა 6G-ში. მისი უზრუნველყოფის პოტენციური გადაწყვეტილებები შეჯამებულია ცხრილში 1.1 და ქვემოთ დეტალურად არის წარმოდგენილი.

1.3.1. ღიაობასთან დაკავშირებული გადაწყვეტილებები

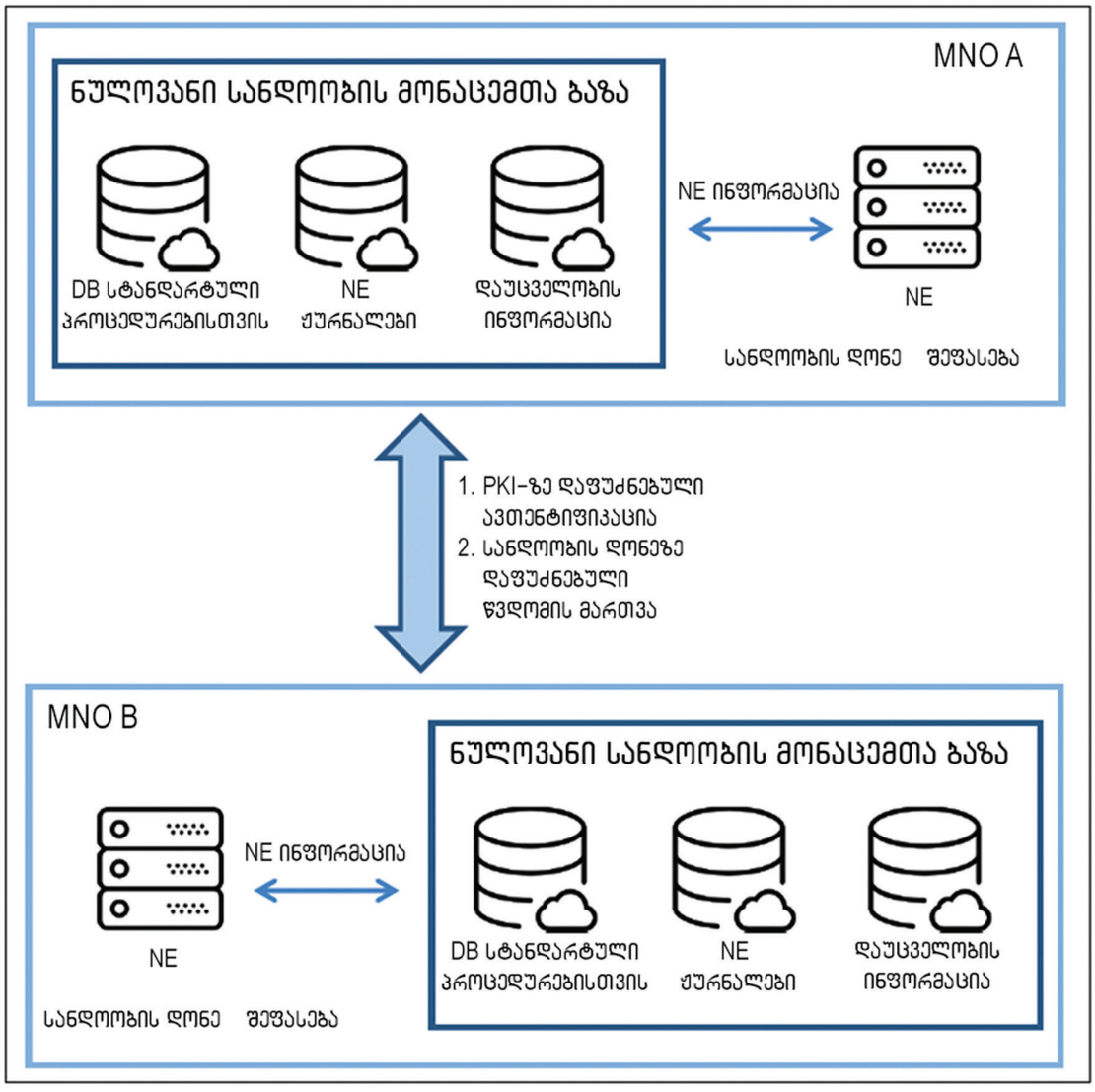
რაც შეეხება ქსელის ღიაობას, ჩვენ წარმოვადგენთ უსაფრთხოების შესაძლო გადაწყვეტილებებს, რომლებიც დაკავშირებულია არქიტექტურის ღიაობასთან და ღია წყაროსთან.

6G სისტემის უსაფრთხოების არქიტექტურა ღიაობისთვის: მოსალოდნელია, რომ 6G გახდება უფრო ღია ქსელი, ვიდრე 5G და ამიტომ, ქსელის შიგნითა და გარეთა ნაწილები სულ უფრო ბუნდოვანი გახდება. აქედან გამომდინარე, ძნელია გამოიყენო არსებული, პერიმეტრზე დაფუძნებული ქსელის უსაფრთხოების მეთოდები, როგორიცაა: IPSec, firewall და IDS, რომლებიც განასხვავებენ შიდა და გარე ნაწილებს და უსაფრთხოებას სასაზღვრო წერტილში იყენებენ. პერიმეტრზე დაფუძნებული ქსელის უსაფრთხოების ასეთი შეზღუდვის შესამცირებლად, 6G უსაფრთხოების არქიტექტურამ მხარი უნდა დაუჭიროს მობილურ საკომუნიკაციო ქსელში ნულოვანი სანდოობის (ZT) უსაფრთხოების პრინციპს.

ZT არის უსაფრთხოების პარადიგმა, რომელიც ორიენტირებულია სისტემის რესურსების დაცვაზე. ZT ვარაუდობს, რომ თავდამსხმელი შეიძლება არსებობდეს ქსელის შიგნით და ქსელის ინფრასტრუქტურა ხელმისაწვდომი ან არასანდოა გარედან. ამდენად, აუცილებელია მუდმივად შეფასდეს შიდა აქტივების სანდოობა საფრთხეების მიმართ და დამცავი ზომების გამოყენება რისკების შესამცირებლად. ZT არქიტექტურა არის უსაფრთხოების არქიტექტურა, რომელიც იყენებს ZT კონცეფციას და მოიცავს ურთიერთობებს NE-ებს, პროტოკოლის პროცედურებსა და წვდომის პოლიტიკას შორის. ამიტომ, ZT არქიტექტურა უნდა იყოს უსაფრთხოების ძირითადი პრინციპი 6G უსაფრთხოების არქიტექტურაში, რომელშიც სხვადასხვა ფორმა-ფაქტორი სხვადასხვა სანდოობით წვდება ქსელს და მესამე მხარეს აქვს წვდომა ქსელის მონაცემებსა და მომხმარებლის ინფორმაციაზე ქსელში, რათა გააუმჯობესოს QoS თითოეული სერვისისთვის და QoE – თითოეული მომხმარებლისთვის.

ZT არქიტექტურის სტრუქტურის მიხედვით, პირველ რიგში, თითოეულმა NE-მ უნდა მოახდინოს ორმხრივი ავთენტიფიკაცია სხვა NE-ებთან უსაფრთხო გზით, როგორიცაა საჯარო გასაღების ინფრასტრუქტურა (PKI). გარდა ამისა, NE-ები მუდმივად აანალიზებენ UE/RAN/NF-ების ქცევას და ადგენენ, არის თუ არა ის არანორმალური. ამ ქცევითი ანალიზის საფუძველზე, თითოეული NE აფასებს სხვა NE-ების სანდოობის დონეს (TL). NE-ებმა უნდა განახორციელონ წვდომის კონტროლი, რათა დაიცვან შიდა ქსელები და აბონენტების ინფორმაცია არაავთენტიფიცირებული, არასანდო ან არანორმალური NE-ების წვდომისგან.

TL-ის შესაფასებლად აუცილებელია ყველა ინფორმაციის შეგროვება და DB-ში შეყვანა. მაგალითად, 6G სისტემამ უნდა შექმნას სტანდარტული სტატუსის DB თითოეული NE-სთვის, აგენერიროს შეტყობინებები, რომლებიც შეიძლება გადაიცეს თითოეულ სტატუსში და შეაგროვოს სტატუსის ინფორმაცია, შეტყობინებები თითოეულ NE-ზე, როგორიცაა წარსულის ისტორია და HW/SW დაუცველობის ინფორმაცია. თითოეული NE-ის და DB-ის შესახებ ინფორმაციის გაანალიზებით, 6G სისტემას შეუძლია შეაფასოს თითოეული NE-ის TL, როგორც ეს ნაჩვენებია ნახ. 1.3-ზე.



ნახ. 1.3. ნულოვანი სანდოობის კონცეფციის ილუსტრაცია

UE-ის TL-ის შეფასების კონკრეტულ მაგალითად შეიძლება ჩაითვალოს UE-ის მდგომარეობა და მისი ქცევა. დავუშვათ, RAN იღებს რადიორესურსების მართვის (RRC) კავშირის განახლების შეტყობინებას UE-დან RRC კავშირის უქმ მდგომარეობაში. 3GPP სტანდარტული პროცედურის გათვალისწინებით, ქცევა არანორმალურია. ამიტომ, RAN-ს შეუძლია შეაფასოს TL, როგორც დაბალი. სტანდარტული პროცედურებისა და UE-ის ოპერაციების ამ გზით ანალიზით, სისტემამ შესაძლოა აღმოაჩინოს მავნე UE-ები, რომლებმაც შეიძლება სცადონ DoS-ის გამოწვევა ან გაანალიზონ დაუცველობა სისტემაში ანომალიური შეტყობინებების გადაცემით.

ერთი NE-სთვის ძალიან ძვირია DB-ის და სისტემის შექმნა ყველა სხვა NE-ის TL-ის შესაფასებლად. აქედან გამომდინარე, საჭიროა პროცედურა და სისტემა, რათა ეფექტიანად შეფასდეს TL მთელ სისტემაში და უსაფრთხოდ გაზიარდეს TL NE-ებს შორის, რომლებსაც აქვთ ორმხრივად დაცული საიმედოობა.

გარდა ამისა, ინტერფეისები, როგორიცაა: EAP-TLS, SEPP და CAPIF, შეიძლება გამოაშკარავდეს ან გატეხილი იყოს მავნე ან კომპრომეტირებული ოპერატორების გამო. თუ TL-ის შეფასება არ არის მოწოდებული ან TL არ იქნება სათანადოდ შეფასებული, არასანდო NE-ებს შეუძლიათ წვდომა მიიღონ პერსონალურ ინფორმაციაზე ან სცადონ სისტემაზე თავდასხმა. ამიტომ, TL-ზე დაფუძნებული სანდოობის ქსელი საჭიროა მობილურ ქსელებსა და საჯარო მონაცემთა ქსელებს შორის კავშირისთვის.

ღია წყაროს უსაფრთხოების მართვის ავტომატიზებული სისტემა: ღია წყაროს უსაფრთხოების პრობლემის გადასაჭრელად ყველაზე მნიშვნელოვანია მართვის ავტომატიზებული სისტემის გამოყენება 6G სისტემის განვითარების პერიოდში, რომელიც მართავს დაუცველობებს ღია წყაროების დანერგვის, გამოყენების, განახლებისა და წაშლის შედეგად. თავდაპირველად, ღია წყაროს კოდის გამოყენებისას, ყველა ინფორმაცია, სახელის, ვერსიის და ჩამოტვირთვის ადგილის ჩათვლით, უნდა ჩაიწეროს. ასევე აუცილებელია DB-ის შექმნა, რომელიც ინახავს ღია წყაროს დაუცველობას და მათ პატჩებს. გარდა ამისა, დაუცველობის აღმოსაჩენად და პატჩების უზრუნველსაყოფად საჭიროა მართვის ავტომატიზებული სისტემა, რათა სწრაფად შემოწმდეს და გასწორდეს დაუცველობა. დაბოლოს, უნდა დაინერგოს უსაფრთხო უსადენო პროცედურა, რათა პატჩებიანი SW დროულად იქნეს გამოყენებული.

გარდა ამისა, უსაფრთხოების მართვის სისტემა სპეციალური ორგანიზაციის მეშვეობით უნდა იყოს დანერგილი, რათა მართოს ღია წყაროს დაუცველობა, გამომდინარე როგორც გრძელვადიანი პერსპექტივიდან, ასევე ცვლილებებიდან დეველოპერების აღქმაში და შემუშავებული უსაფრთხოების გადაწყვეტილებებიდან.

1.3.2. AI უსაფრთხოების ტექნოლოგიები

მომხმარებლებისა და სისტემების AML-ისგან დასაცავად, უზრუნველყოფილი უნდა იყოს გამჭვირვალობა, რომელიც ამოწმებს, რამდენად უსაფრთხოდ მოქმედებენ AI სისტემები AML-ის წინააღმდეგ. პირველ რიგში, AI მოდელები საიმედო სისტემაში უნდა შეიქმნას. ასევე საჭიროა ისეთი პროცედურის გატარება, როგორიცაა ციფრული ხელმოწერა, რათა შემოწმდეს, არის თუ არა AI მოდელები, რომლებიც მუშაობენ UE-ში, RAN-ში და Core-ში ბოროტად მოდიფიცირებული ან მავნე თავდასხმის შედეგად შეცვლილი. შესაბამისად, თუ მავნე AI მოდელი დაფიქსირდა, სისტემამ უნდა შემოიტანოს თვითგანკურნების ან აღდგენის პროცედურები.

ასევე საჭიროა AML-ის წინააღმდეგ მდგრადი AI-ის შემუშავება. მოდელის ინვერსიით თავდასხმისგან თავის დასაცავად, AI მოდელი უნდა შეიქმნას და გავრცელდეს ისე, რომ კონფიდენციალურობის შესახებ ინფორმაციის ამოღება, როგორიცაა UE მობილურობის ინფორმაცია, მომხმარებლის აპლიკაციის გამოყენების ინფორმაცია და ძიების ისტორია, შეუძლებელი იყოს AI მოდელიდან, შესაბამისი ხმაურის დამატებით კონფიდენციალურობის ინფორმაციაზე. მონაცემთა მოწამვლის თავდასხმის საწინააღმდეგოდ, NE-ებმა უნდა დაატრენინგონ AI მოდელი სანდო NE-ებიდან შეგროვებული მონაცემებით. ალტერნატიულად, NE-ებს შეუძლიათ გამორიცხონ გარკვეული ტრენინგის მონაცემები ყველა შესაძლებელი ტრენინგის მონაცემების ერთობლიობიდან შეგროვებული მონაცემების განაწილების საფუძველზე.

მოდელიდან არიდების ტიპის თავდასხმის შემთხვევაში შესაძლებელია შემოწმდეს, არის თუ არა შემავალი მონაცემები ზოგად სტატისტიკურ დიაპაზონს მიღმა ან არის თუ არა შემავალი და გამომავალი მონაცემები ქსელის ნორმალურ დიაპაზონს მიღმა. მაგალითად, AI-ზე დაფუძნებული გადაცემის შემთხვევაში, RAN ირჩევს HO-ს, გაზომვის ანგარიშების კორელაციის ან სტატისტიკური დიაპაზონის, ასევე გაზომვის ანგარიშის საფუძველზე.

AI მოდელის კონფიდენციალურობის უზრუნველსაყოფად, NE-ებს შეუძლიათ დააყენონ ზღურბლური მნიშვნელობა, შეყვანის მოთხოვნების რაოდენობის მიხედვით, რომელიც აკმაყოფილებს AI მოდელის მიზანს. თუ ზღურბლზე მეტი მნიშვნელობის შეყვანის მოთხოვნაა გადაცემული, NE-ებს შეუძლიათ განსაზღვრონ ანომალიის გამოვლენა ისე, რომ მოდელის მოპოვების თავდასხმა დაიბლოკოს. ალტერნატიულად, NE-ებს შეუძლიათ გამოავლინონ მოდელის მოპოვების მცდელობები ნორმალური განაწილებიდან თანმიმდევრული მოთხოვნების განაწილების ანალიზით.

1.3.3. კონფიდენციალურობის შემანარჩუნებელი გადაწყვეტილება

მომხმარებლის პერსონალური ინფორმაციის უსაფრთხო შენახვისა და გამოყენების მიზნით, უნდა განისაზღვროს ურთიერთშეთანხმებული პროცედურები აბონენტს, MNO-ს და სერვისის პროვაიდერს შორის პერსონალური ინფორმაციის შეგროვების, შენახვის, გამოყენებისა და განკარგვისას. ამ პროცედურების მეშვეობით, 6G სისტემა მინიმუმამდე ამცირებს არასაჭირო პერსონალური ინფორმაციის შეგროვებას, ინახავს პერსონალურ ინფორმაციას სანდო აღსრულების გარემოზე, საიმედო SW-ზე და ახდენს გამჟღავნებული ინფორმაციის მინიმიზაციას ან ანონიმიზაციას პერსონალური ინფორმაციის გამოყენებისას. თუ გამოყენების მიზანი მიღწეულია, ეს ინფორმაცია დაუყოვნებლივ უნდა განადგურდეს. კონკრეტულად, როდესაც MNO ან სერვისის პროვაიდერი იყენებს ინფორმაციას პერსონალიზებული QoS-ის და QoE-ის გასაუმჯობესებლად, მომხმარებელს უნდა ეცნობოს და სტანდარტული პროცედურების მეშვეობით თანხმობა იქნეს მიღებული.

პერსონალური ინფორმაციის მიწოდებისას, MNO-მ უნდა გადაამოწმოს სათანადო ავთენტურობა და უფლებამოსილება. გარდა ამისა, მომხმარებლის ინფორმაციის გამოყენებისა და ანალიზის დროს უნდა მოხდეს მისი ანონიმიზაცია კონფიდენციალურობის დასაცავად ან ის უნდა დაიშიფროს ჰომომორფული დაშიფვრით, რათა მონაცემები ხელმისაწვდომი გახდეს დაშიფრული ფორმით. AI-ზე დაფუძნებული გადაწყვეტილება, როგორიცაა სწავლებაზე დაფუძნებული კონფიდენციალურობის ინფორმირებულობის გადმოტვირთვის სქემა, ასევე შეიძლება გამოყენებულ იქნეს როგორც მომხმარებლის ადგილმდებარეობის კონფიდენციალურობის, ასევე გამოყენების მოდელის კონფიდენციალურობის დასაცავად. UE იდენტიფიკატორების (როგორიცაა: RNTI, GUTI, მობილური აბონენტის დროებითი იდენტიფიკაცია და მობილური მოწყობილობის საერთაშორისო იდენტიფიკაცია (IMEI)) უსაფრთხოდ შექმნით და შემთხვევითი გადანაწილებით, სისტემას ასევე შეუძლია დაიცვას მომხმარებლის მდებარეობა ან მომსახურების ისტორია თავდამსხმელებისგან.

დაბოლოს, 6G-მ უნდა მოიცვას მომხმარებელთა ინფორმაციის შეგროვების, შენახვის, მართვისა და განკარგვის პროცედურები მთავრობის მიერ მიღებული კანონების დაცვით.

1.3.4. გადაწყვეტილება ვირტუალიზაციის/კონტეინერიზაციის უსაფრთხოებისთვის

ვირტუალიზაციის/კონტეინერიზაციის უსაფრთხოების სხვადასხვა საკითხთან დაკავშირებით უნდა დაინერგოს შემდეგი ტექნოლოგიები:

თუ ჰიპერვიზორი კომპრომეტირებულია, vRAN/vCore ასევე კომპრომეტირებულია. ამრიგად, vRAN/vCore-მა უნდა იმოქმედოს მხოლოდ უსაფრთხო ვირტუალიზაციის ფენით აღჭურვილ სისტემაზე. კერძოდ, ვირტუალიზაციის ფენა მოიცავს უსაფრთხოების ტექნოლოგიას, რომელიც აღმოაჩენს ფარულ მავნე კოდებს, როგორიცაა მაგალითად, Rootkit. მან უნდა ისარგებლოს უსაფრთხო HW-თი, რათა უზრუნველყოს ვირტუალიზაციის ფენის მთლიანობა, როგორც სანდო პლატფორმის მოდული (TPM).

გარდა ამისა, ჰიპერვიზორმა უნდა უზრუნველყოს სხვადასხვა vRAN/vCore-ის გამოთვლის, შენახვისა და ქსელის სრული იზოლაცია. ჰიპერვიზორმა არა მხოლოდ უნდა დაბლოკოს არაავტორიზებული წვდომა სხვა VM-ებზე, არამედ უნდა შეინახოს vRAN/vCore-ის მონაცემები დაშიფრული გზით. გარდა ამისა, ვირტუალიზაციის ფენამ უნდა გამოიყენოს TLS, უსაფრთხო გარსი (SSH), ვირტუალური კერძო ქსელი (VPN) და ასე შემდეგ, რათა დაიცვას კომუნიკაცია vRANs/vCores-ებს შორის იმავე ვირტუალიზაციის სისტემაში.

გარდა ამისა, ჰიპერვიზორი აღჭურვილი უნდა იყოს IDS/IPS/firewall-ით, რათა გაანალიზოს VM-ის შიდა მდგომარეობა და აღმოაჩინოს შეჭრა, რომელსაც ეწოდება ვირტუალური მანქანის თვითანალიზი (VMI). VMI აანალიზებს და ამოიცნობს საფრთხეებს ვირტუალური CPU რეგისტრის ინფორმაციის, ვირ-

ტუალური მეხსიერების მონაცემების, ფაილის შემავალი/გამომავალი მონაცემების და თითოეული VM-ის საკომუნიკაციო პაკეტების საფუძველზე. ამრიგად, vRAN/vCore უნდა მუშაობდეს მხოლოდ სანდო VMI-ზე. გარდა ამისა, ცოცხალი მიგრაციის უსაფრთხოების პრობლემების გადასაჭრელად, გამოყენებულ უნდა იქნეს უსაფრთხო ცოცხალი მიგრაციის გადაწყვეტილებები, როგორიცაა ქსელის უსაფრთხოების ძრავის ჰიპერვიზორები (NSE-H), ვირტუალური TPM, ცოცხალი მიგრაციის დაცვის სტრუქტურა და როლებზე დაფუძნებული ცოცხალი მიგრაცია.

კონტეინერიზაციის შემთხვევაში, OS-მა სწორად უნდა დააკონფიგურიროს სხვადასხვა კონტეინერის პრივილეგიები, აკრძალოს ძირითადი სისტემის დირექტორიების დამონტაჟება და პირდაპირი წვდომა მასპინძელი მოწყობილობის ფაილების კონტეინერზე. სოკეტზე პაკეტების დასაცავად, OS-მა ასევე უნდა აკრძალოს დაუცველი ქსელის დაყენება (როგორიცაა ხიდის ტიპის ნაგულისხმევი ქსელი), არასაჭირო პორტი, მასპინძელი ქსელის ინტერფეისის დაყენება და SSH შესრულება კონტეინერში.

1.3.5. პოსტკვანტური კრიპტოგრაფიის დანერგვა

6G სისტემამ უნდა გააუქმოს არსებული სუსტი ასიმეტრიული გასაღების დაშიფვრის ალგორითმები კვანტური გამოთვლების დანერგვით და მიიღოს პოსტკვანტური კრიპტოგრაფია (PQC). ბევრი მკვლევარი აქტიურად სწავლობს PQC გადაწყვეტილებებს, მათ შორის გისოსებზე დაფუძნებულ კრიპტოგრაფიას, კოდზე დაფუძნებულ კრიპტოგრაფიას, მრავალგანზომილებიან პოლინომიურ კრიპტოგრაფიას და ჰეშზე დაფუძნებულ ხელმოწერას. აშშ-ის სტანდარტებისა და ტექნოლოგიების ეროვნული ინსტიტუტი (NIST) ხელმძღვანელობს PQC-ის სტანდარტიზაციას და 2016 წელს წამოიწყო პროცესი PQC ალგორითმების მოთხოვნის, შეფასებისა და სტანდარტიზაციისთვის. დაგეგმილია, რომ NIST შეარჩევს შესაბამის PQC ალგორითმებს 2024 წლამდე.

აღსანიშნავია, რომ გასაღებების სიგრძე, რომლებიც ამჟამად განიხილება, როგორც PQC კანდიდატები, რამდენჯერმე აღემატება კრიპტოსისტემებში ფართოდ გამოყენებული არსებული რივესტ-შამირ-ადლემანის (RSA) ალგორითმის 1000 ბიტს. მოსალოდნელია, რომ PQC-ის გამოთვლითი ოვერჰედი უფრო დიდი იქნება, ვიდრე არსებული RSA ალგორითმის. ამიტომ, აუცილებელია PQC-ის სათანადოდ დანერგვა 6G ქსელის HW/SW მუშაობისა და მომსახურების მოთხოვნებით.

1.4. პირველი თავის დასკვნა

ამ თავში ჩვენ წარმოვადგინეთ ტექნოლოგიური ტენდენციები, საფრთხეები და გადაწყვეტილებები 6G უსაფრთხოებისთვის. პირველ რიგში, ჩვენ გამოვავლინეთ და განვიხილეთ მეგატენდენციები, რომლებიც პირდაპირ გავლენას ახდენს უსაფრთხოებასა და კონფიდენციალურობაზე, მათ შორის: ქსელის ღიაობაზე, AI-ზე, კონფიდენციალურობის დაცვაზე, ვირტუალიზაცია/კონტეინერიზაციაზე და კვანტურ გამოთვლებზე; შემდეგ ჩვენ გავაანალიზეთ ამ ტექნოლოგიების დანერგვით გამოწვეული პოტენციური ახალი საფრთხეები და წარმოვადგინეთ შესაძლო გადაწყვეტილებები ამ საფრთხეების მოსაგვარებლად. სანდოობის უზრუნველყოფის სპეციფიკური გადაწყვეტილებების სახით, დეტალურად განვიხილეთ ნულოვანი სანდოობის უსაფრთხოება და ღია წყაროს მენეჯმენტი ქსელის ღიაობისთვის, AI-ის მუშაობის სანდოობის უზრუნველყოფა, თანხმობის პროცედურების და დაშიფვრის ტექნიკის გამოყენება კონფიდენციალურობის დასაცავად და ჰიპერვიზორისა და კონტეინერის უსაფრთხოებისთვის, PQC-ის დანერგვა. იმის გათვალისწინებით, რომ სანდოობა გახდება მნიშვნელოვანი მოთხოვნა 6G-სთვის, შეგვიძლია ვივარაუდოთ, რომ 6G განვითარდება როგორც ყველაზე უსაფრთხო მობილური საკომუნიკაციო ტექნოლოგია.

თავი 2. კონტექსტით გაცნობიერებული უსაფრთხოება და უსაფრთხოების ხარისხის კონტროლი 6G ქსელებისთვის

2.1. შესავალი

ამჟამად მიმდინარეობს ინტენსიური დისკუსიები 6G რადიოკომუნიკაციების მდგრადობასა და სანდოობასთან დაკავშირებით, რაც მიზნად ისახავს 6G უსადენო წვდომისთვის გათვალისწინებული უსაფრთხოების გარანტიების გაძლიერებას. აღსანიშნავია, რომ ზოგიერთი ბოლოდროინდელი, სულ უფრო დახვეწილი თავდასხმა უსადენო პერიფერიაზე (მაგალითად, ჩახშობა ან ყალბი საბაზო სადგურები) შეიძლება განხორციელდეს საკმაოდ მარტივად და დიდი ფინანსური დანახარჯების გარეშე, იაფი SW-ით განსაზღვრული რადიოსისტემების გამოყენებით. გარდა ამისა, ჩვენ ვხედავთ თავდასხმის ზედაპირის გაფართოებას AI-ის და მანქანური სწავლების (ML) საშუალებებით. პარალელურად, როდესაც თანდათან ვშორდებით კლიენტ-სერვერის სტანდარტული ქსელის პარადიგმას და შევდივართ ჭეშმარიტად ბოლო პუნქტების დამაკავშირებელი (E2E) QoS-ის ახალ ეპოქაში, უახლოეს მომავალში მოსალოდნელი იქნება სერვისის დონის შეთანხმებების (SLA) გაჩენა, რომელიც უნდა მოიცავდეს გარანტიებს QoSec-ის შესახებ. ამჟამად QoSec-ის კომპონენტების განმარტება კვლევის პროცესშია: როგორ განვსაზღვროთ უსაფრთხოების საჭირო დონე და შევთავაზოთ ადაპტიური, დინამიკური და რისკის მიხედვით გაცნობიერებული უსაფრთხოების გადაწყვეტილებები.

იმავდროულად, მოსალოდნელია, რომ 6G სისტემების ევოლუცია დანერგავს სიტუაციური ცნობიერების მიღწევის ახალ საშუალებებს საკომუნიკაციო „კონტექსტის“ აღბეჭდვითა და ინტერპრეტაციით, რომელიც სხვასთან ერთად მოიცავს ქსელურ ტომოგრაფიას, კვანძების შეზღუდვებს და ინფორმაციის ასაკს. პროგნოზირებულია, რომ QoSec-ში კონტექსტური ცნობიერების ჩართვა უზრუნველყოფს რისკის ან საფრთხის დონის და უსაფრთხოების დონის ასპექტების უფრო ეფექტიან მართვას, განსაკუთრებით ისეთი აპლიკაციებისთვის, რომლებსაც აქვთ უსაფრთხოების არაფუნქციური მოთხოვნები, როგორიცაა: ავტონომიური მანქანები, ჯგუფურად და მოწესრიგებულად გადაადგილებადი ავტოკოლონები და ელექტრონული ჯანმრთელობა.

ამ სტრუქტურაში უსაფრთხოების კონტროლის ჩართვა, ფიზიკური ფენის უსაფრთხოების (PLS) პალიტრიდან შეიძლება, განსაკუთრებით მიმზიდველი იყოს მისი დაბალი გამოთვლითი სირთულის (შესაბამისი დანერგვები დაფუძნებულია სტანდარტულ კოდერებზე) და თანდაყოლილი უნარის გამო, მოახდინოს ადაპტირება გადამცემი გარემოს თვისებებთან. PLS-ის ჩართვა 6G უსაფრთხოებაში მოითხოვს კონტექსტის შესახებ ცნობიერების გაზრდას და შეიძლება იყოს განსაკუთრებით მიმზიდველი მასობრივი მანქანის ტიპის კომუნიკაციებისთვის (mMTC) და ულტრა დაბალი შეყოვნების გამოყენების შემთხვევებისთვის.

ამ თავის დანარჩენ ნაწილს ჩვენ დავიწყებთ 5G-ში უსაფრთხოების ღია საკითხების განხილვით და 6G-ის წინაშე მდგარი გამოწვევების შესწავლით, შემდეგ კი გადავალთ ამ გამოწვევების გადასაჭრელად გზამკვლევი რუკის წარმოდგენაზე. ზოგიერთი შემოთავაზებული იდეის საილუსტრაციოდ, ჩვენ გამოვყოფთ სიცოცხლისუნარიან გადაწყვეტილებებს 5G და 6G უსაფრთხოების სპეციფიკური დაუცველობის აღმოსაფხვრელად და დასკვნების გაკეთებამდე განვიხილავთ შესაძლო სამომავლო მიმართულებებს.

2.2. 5G უსაფრთხოების ღია საკითხები და უსაფრთხოების კვლევების გამოწვევები 6G-სთვის

წინა თაობებთან შედარებით, 5G უსაფრთხოების პროტოკოლების გაუმჯობესების მიუხედავად, ჯერ კიდევ არსებობს ღია საკითხები, რომლებიც არ არის სრულად მოგვარებული (მაგალითად, თავდასხმები ყალბი საბაზო სადგურების ზოგადი ქოლგის ქვეშ). პარალელურად, 6G ევოლუციის გზაზე, უსაფრთხოების ახალი გამოწვევები წარმოიქმნება ძირითადი საოპერაციო პარამეტრების ფუნდამენტური ცვლილებების შედეგად:

- დასაშვები E2E შეყოვნება.
- ქსელების დიდი მასშტაბები mMTC გამოყენების შემთხვევაში და ძალიან ფართომასშტაბიანი IoT.
- განლაგებული IoT მოწყობილობების (განსაკუთრებით სენსორების) ხანგრძლივი სიცოცხლის პერიოდი, რომელიც უნდა იყოს დაცული.
- გამოყენებული ჰეტეროგენული რადიოსიხშირული ტექნოლოგიების მრავალფეროვნება.
- კვანტური კომპიუტერების ცხოვრებაში დანერგვისკენ გადადგმული დაჩქარებული ნაბიჯები.

ქვემოთ ჩატარებულია მოკლე მიმოხილვა 5G-ში უსაფრთხოების ღია საკითხების და 6G-ის ევოლუციაში უსაფრთხოების ზოგიერთი გამოწვევის შესახებ. ეს დისკუსია იძლევა მოტივაციას, უსადენო ქსელების მომავალი თაობისთვის, კონტექსტით გაცნობიერებული უსაფრთხოების ჩვენი გადაწყვეტილებების შესახებ. აღსანიშნავია, რომ ეს ქსელები ასევე შეძლებენ ფიზიკური ფენის გამოყენებას მოქნილი და ადაპტირებული უსაფრთხოების კონტროლის უზრუნველსაყოფად.

ტერმინი „ყალბი საბაზო სადგურები“ (FBS) აღწერს ნამდვილ საბაზო სადგურებზე იმიტირებულ თავდასხმებს. ამ თემას ამჟამად სწავლობს 3GPP-ის SA3 სამუშაო ჯგუფი, როგორც ეს დოკუმენტირებულია ტექნიკურ ანგარიშში (TR) TR 33.809-ში. როგორც წესი, 5G-ში, FBS არის „კაცი შუაში“ (MitM) ან ძალიან შეუმჩნეველი ჩამხშობი. ძირითადი დაუცველობა, რომელიც დაფიქსირებულია FBS-ების მიერ, არის ის, რომ ქსელში შესვლის ფაზები, რომლებიც წინ უძღვის 5G უსაფრთხოების პროტოკოლების ამოქმედებას, განსაკუთრებით კრიტიკულია TR 33.809-ში აღწერილი მრავალი თავდასხმისთვის. მაგალითად, თავდასხმებს, რომლებიც გენერირდება სასიგნალო ინფორმაციის გადამცემი არხების შეცვლილი ვერსიების გამოყენებით, შეიძლება ჰქონდეს დამღუპველი შედეგები ფიჭის ყველა ტერმინალისთვის, შეაფერხოს ქსელთან მათი დაკავშირება ან აიძულოს ისინი, რომ დეგრადირებულ რეჟიმში იმუშაონ. შედეგად, აუცილებელია შემოთავაზებული იქნეს მეთოდები, რომლებიც UE-ს საშუალებას მისცემს განსაზღვროს, არის თუ არა BS ლეგიტიმური, არაავთენტიფიცირებული შეტყობინებების გაცვლამდე. ამ მიზნით, PLS შეიძლება გამოყენებულ იქნეს BS-ის ლოკალიზაციის ჩართვის მიზნით UE-ის მიერ, როგორც რბილი ავთენტიფიკაციის ფაქტორი.

კრიტიკული ულტრა საიმედო დაბალი შეყოვნების კომუნიკაციები (URLLC) ჩვეულებრივ გამოიყენება IIoT-ის, მანქანა-ყველაფერთან და სხვა აპლიკაციებისთვის, რომლებიც საჭიროებენ დაბალ შეყოვნებას და ძალიან მაღალ საიმედოობას. მაღალი საიმედოობის მისაღწევად შესაძლო გზაა მრავალფეროვნების გაზრდა (მაგალითად, შესაძლებელია მრავალი პარალელური ტრანსმისიის გამოყენება). თუმცა, ეს, შესაბამისად, ზრდის „თავდასხმის ზედაპირს“, ამასთან, შეიძლება დააწესოს უფრო მკაცრი შეზღუდვები მთლიანობის შემოწმების სიჩქარის თვალსაზრისით. შეყოვნების კუთხით ზედმეტად აგრესიულმა მიზნებმა შესაძლოა მიგვიყვანოს უსაფრთხოების ახალ არქიტექტურამდე. თანამედროვე

წინადადებებმა სწრაფი ავთენტიფიკაციისთვის, იმპლიციტური სერტიფიკატების ან სერტიფიკატების გარეშე გადაწყვეტილებების გამოყენებით, შეიძლება ავთენტიფიკაცია დააჩქაროს. მიუხედავად ამისა, რჩება მრავალი ღია გამოწვევა ქვემილიწამიანი შეფერხებით შეზღუდული URLLC სისტემებისთვის, რომლებიც შეეხება არა მარტო ავთენტიფიკაციას, არამედ ასევე კონტროლის და მონაცემთა სიბრტყეების მთლიანობას, კონფიდენციალურობას, როგორც ეს დოკუმენტირებულია 3GPP TR 33.825-ში.

მიუხედავად იმისა, რომ მრავალშესასვლელიანი და მრავალგამოსასვლელიანი (MIMO) სისტემები, მათ შორის მასიური MIMO (mMIMO) ართულებს მოსმენას ენერგიის ფოკუსირების გამო, ისინი მაინც აჩენენ დაუცველობის წერტილებს. მართლაც, სხივის ფორმირება mMIMO სისტემებში ეყრდნობა არხის ზუსტ შეფასებას. პილოტ-სიგნალები გადაიცემა არხის მდგომარეობის შესახებ ინფორმაციის (CSI) მისაღებად, რაც თავის მხრივ წინასწარი კოდირების საშუალებას იძლევა. თუ CSI სწორად არ არის შეფასებული (მაგალითად, ინტერფერენციის ან ჩამხშობის მიერ მიზანმიმართული დაბინძურების გამო), წინასწარი კოდერი გაფანტავს ენერგიას, რაც პოტენციურ გაჟონვას და ლინკის ცუდ ხარისხს გამოიწვევს. ამ უკანასკნელს მივყავართ სერვისის მიუწვდომლობამდე, რაც DoS ტიპის თავდასხმას იწვევს. მსგავსი თავდასხმები ასევე შეიძლება განხორციელდეს გარემოს წვდომის კონტროლზე (MAC) მოწყობილობების მიერ გაგზავნილი CSI ანგარიშების გაყალბებით. შედეგად, ქსელში შესვლისას, სხივის მართვის ფაზა დაუცველია რადიოსიხშირული (RF) ჩამხშობების თავდასხმების მიმართ. ამიტომ, გადამწყვეტი მნიშვნელობა აქვს ისეთი საშუალებების ქონას, რომლებიც აღმოაჩენენ ჩამხშობებს, მოახდენენ მათ ლოკალიზაციას და ნეიტრალიზაციას, დანერგავენ მათ შემასუსტებელ გადაწყვეტილებებს.

მიუხედავად იმისა, რომ 5G მოიცავს ღონისძიებების ერთობლიობას კონფიდენციალურობის გასაუმჯობესებლად მომხმარებლის იდენტურობის თვალსაზრისით, მომხმარებლის ადგილმდებარეობის კონფიდენციალურობისა და მომხმარებლის მიუკვლევადობის შესახებ ბოლოდროინდელმა კვლევამ აჩვენა, რომ ჯერ კიდევ ბევრი ღია საკითხია შესასწავლი, მაშინ, როდესაც კონფიდენციალურობის გარანტიები საკმაოდ სუსტია გამომდინარე საბოლოო მომხმარებლის პერსპექტივიდან. მომავალი მობილური ქსელების მიერ დამუშავებული პერსონალური მონაცემების რაოდენობა არსებითად გაზრდის სამთავრობო უწყებების, ისევე როგორც მოწინააღმდეგე სუბიექტების რაოდენობას, რომლებსაც პოტენციურად მაღალი ინტერესი აქვთ ასეთი მონაცემების მიმართ; მომავალი უსადენო ქსელები შექმნილი უნდა იყოს ისე, რომ უზრუნველყოს კონფიდენციალურობა ოპერატორებისადმი ნდობის გარეშე.

კიდევ ერთი გამოწვევა მომდინარეობს კვანტური გამოთვლებიდან, რომელმაც მნიშვნელოვანი პროგრესი განიცადა დიდი რაოდენობის ადრეული ინვესტიციების შემდეგ. ვინაიდან 5G-ში გამოყენებული ზოგიერთი ყველაზე მნიშვნელოვანი კრიპტოგრაფიული ალგორითმი არ არის კვანტური გამოთვლების მიმართ რეზისტენტული, შესაბამისი პროტოკოლები პოსტკვანტური კრიპტოალგორითმების გამოყენებით უნდა გადაკეთდეს. NIST ამჟამად აფასებს ახალ პოსტკვანტურ კრიპტოალგორითმებს, რათა შეცვალოს ამჟამად გამოყენებული საჯარო გასაღების დაშიფვრის სქემები. თუმცა, არსებობს ზოგადი შეშფოთების საფუძველი, რომ კვანტური წინააღმდეგობა, სულ მცირე, უახლოეს მომავალში ახალი კრიპტოგრაფიული სისტემების სირთულის ზრდას გამოიწვევს. მაგალითად, გასაღების უფრო დიდი ზომები შეიძლება წარმოადგენდეს მნიშვნელოვან პრაქტიკულ პრობლემას. ეს შეიძლება იყოს განსაკუთრებით რთული URLLC-სთვის, დაბალი სიმძლავრის და დაბალფასიანი მოწყობილობებისთვის, რაც კიდევ უფრო ამძაფრებს კონფლიქტურ ტენდენციებს მომავალ სისტემებში და საჭიროებს ურთიერთკომპრომისს გამოთვლებზე დაფუძნებულ კრიპტოგრაფიასა და დაბალფასიანი მოწყობილობებისთვის რეალურ დროში კომუნიკაციას შორის.

არსებობს უსაფრთხოების მრავალი გამოწვევა, რომელიც წარმოიქმნება ძალიან ფართომასშტაბიანი, გრძელვადიანი, შეზღუდული IoT ქსელების დანერგვით. ნაკლებად სავარაუდოა, რომ აბონენტის

იდენტიფიკაციის მოდულის (SIM) ბარათის გარეშე ფუნქციონირებად დაბალფასიან IoT მოწყობილობებს შეეძლოთ უსაფრთხოების მოწინავე მექანიზმების მხარდაჭერა გამოთვლითი სიმძლავრის, მეხსიერების და ალბათ, რაც ყველაზე რთულია, ენერგიის მოხმარების შეზღუდვების გამო. მიუხედავად იმისა, რომ „მსუბუქი“ კრიპტოგრაფია შეიძლება ზოგიერთი პრობლემის გადაჭრაში დაგეხმაროს, ასეთი ალგორითმები ამჟამად არ არის 5G-ის ნაწილი და „მსუბუქი“ პოსტკვანტური გადაწყვეტილებების შემუშავება ახლანდელი კვლევების სფეროა.

გარდა ამისა, B5G ქსელთან დაკავშირებული IoT მოწყობილობების დიდი რაოდენობა (ტრილიონი) ქმნის დიდ გამოწვევებს ინფორმაციის უსაფრთხოების მართვის თვალსაზრისით, მაგრამ ასევე, თვითონაც წარმოადგენს უსაფრთხოების რისკს, როგორც ეს აჩვენა 2016 წლის მირაის (Mirai) თავდასხმამ, მძიმე საერთო შედეგებით. ამ ასპექტში მნიშვნელოვანი ხდება დეცენტრალიზებული შეჭრის/ანომალიის გამოვლენა.

კიდევ ერთი მნიშვნელოვანი ფაქტორია ის, რომ ბევრ IoT მოწყობილობას, როგორც წესი, ექნება სიცოცხლის ძალიან დიდი ხანგრძლივობა (ათზე მეტი წელი ლეპტოპის სამი წლისგან განსხვავებით) და შეიძლება განაწილდეს დიდ გეოგრაფიულ ზონებში. ძნელია იმის გარანტირება, რომ მასობრივად წარმოებულ, გამოთვლებითა და ენერგეტიკით შეზღუდულ IoT მოწყობილობებს ექნებათ აპარატურა, რომელსაც შეუძლია განახლდეს საჭირო პატჩებით, რათა გაუძლოს ყველა საფრთხეს, რომელიც წარმოიქმნება მათი სიცოცხლის განმავლობაში (მაგალითად, პოსტკვანტური წინააღმდეგობა).

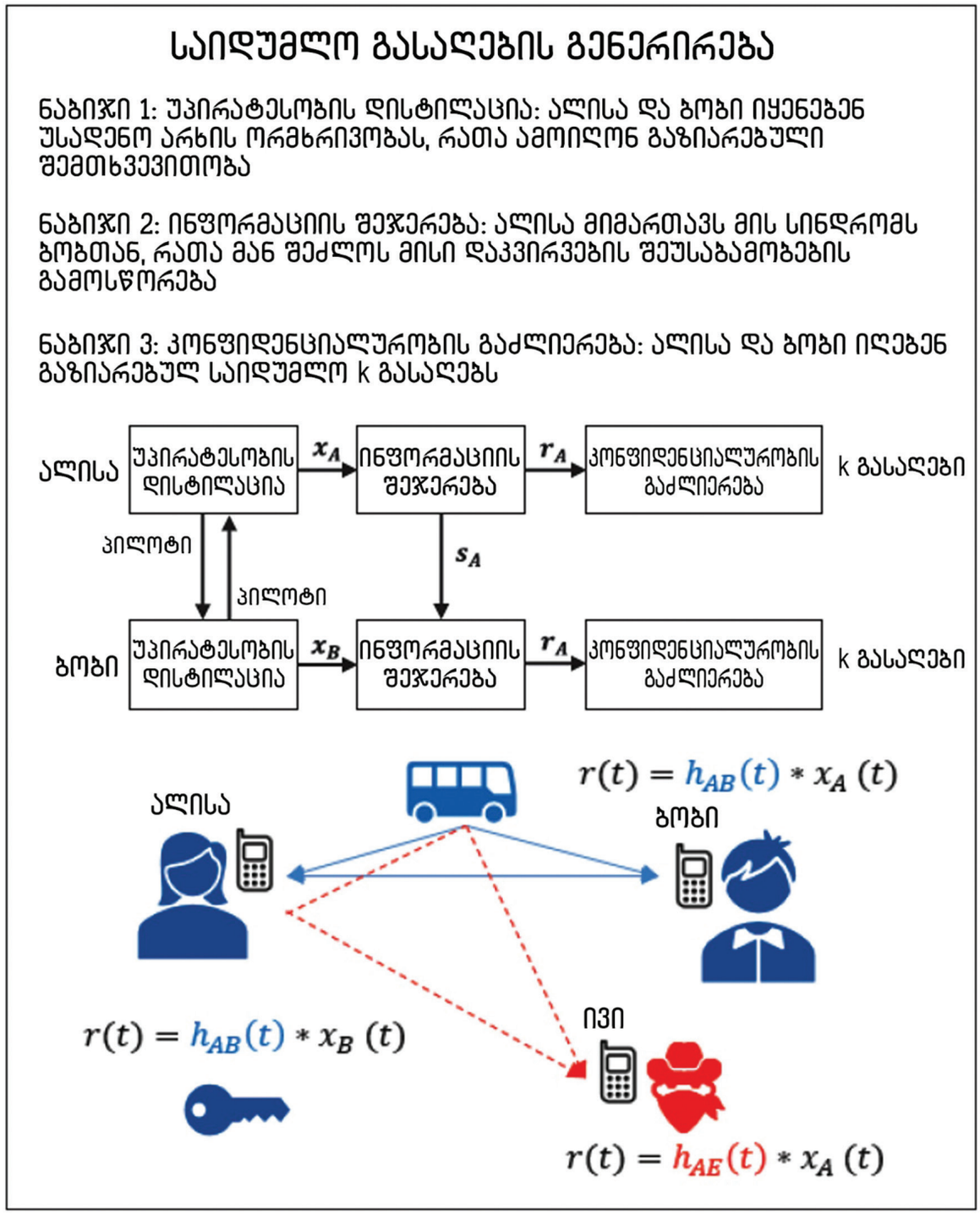
2.3. 6G, როგორც კონტექსტით გაცნობიერებული QoSec-ის დანერგვის საშუალება PLS-ის გამოყენებით

მიუხედავად იმისა, რომ 6G ჯერ კიდევ რამდენიმე წლით არის დაშორებული სტანდარტიზაციისგან, კონსენსუსი იზრდება მისი სავარაუდო ევოლუციის გზაზე, რომელიც ქვემოთ მოკლედ არის აღწერილი.

უფრო მაღალი სიხშირეები და გაზრდილი გამტარუნარიანობა: წინა თაობებში დანახული ევოლუციის გაგრძელებით, 6G გამოიყენებს უფრო მაღალ გადამტან სიხშირეებს და გაზრდილ გამტარუნარიანობას, გადაადგილდება რა 100 გჰც-ზე მეტი სიხშირეებისკენ, რაც იძლევა 1 გჰც-ზე მეტი სიხშირის გატარების ზოლის გამოყოფის საშუალებას. სიხშირის გატარების ფართო ზოლმა შესაძლოა გაზარდოს დაკვირვებადი არხის ენტროპია სიხშირის დომენში, რომელიც პოტენციურად შეიძლება იქნეს გამოყენებული PLS-ის საიდუმლო გასაღების გენერაციაში (SKG) უსადენო არხების კოეფიციენტებზე დაყრდნობით, რომელთა ძირითადი მექანიზმები გამოსახულია ნახ. 2.1-ზე. გარდა ამისა, მილიმეტრული ტალღებისა და სუბტარაჰერცული რადიოსიხშირეების სისტემებში სხივის ფორმირება ძალიან ვიწრო სხივებით ხდება, როგორც შესაძლებლობა, საანტენო მესრებით დაკავებული უფრო მცირე ფართობის და ასევე, როგორც აუცილებლობა არხის უფრო მაღალი მილევის კომპენსაციის საჭიროების გამო. მაღალი მიმართულობის მქონე სხივის ფორმირებამ შეიძლება შეამციროს მოსმენის შესაძლებლობები, როგორც ეს ნაჩვენებია ნახ. 2.2-ზე, მაშინ როდესაც მსგავსი შესაძლებლობები არსებობს ხილული სინათლით კომუნიკაციისთვის (VLC). ამრიგად, 6G mMIMO-ს შეუძლია შემოგვთავაზოს სიცოცხლისუნარიანი სცენარი მოსმენის არხის გამოყენების შემთხვევისთვის.

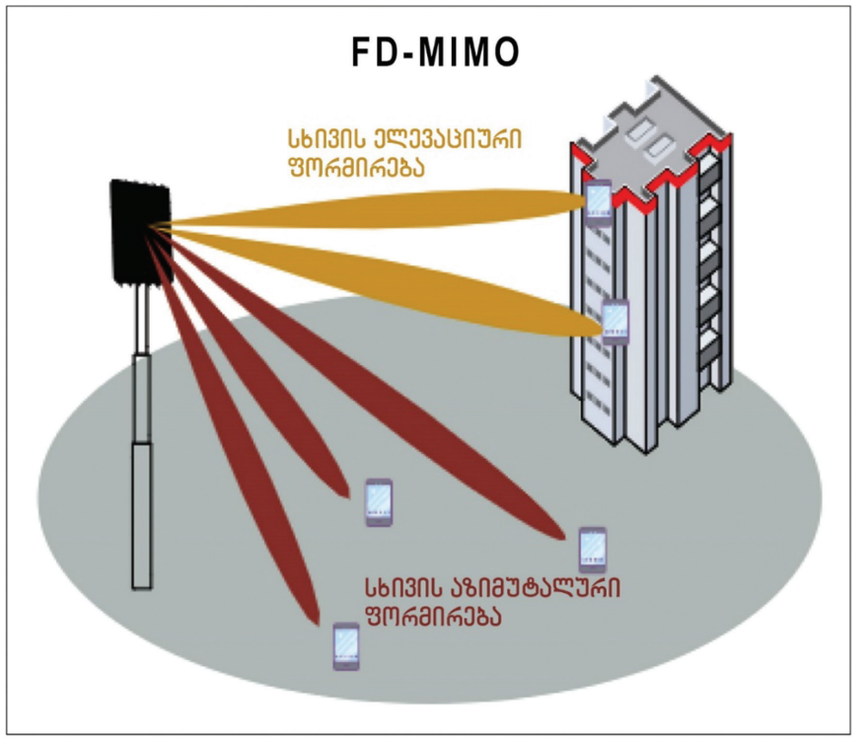
ინტეგრირებული ზონდირება და კომუნიკაციები: გარდა მაღალი გარჩევადობის გამოსახულების, ვიდეოს, ხმის, სხვა შესაძლო ზონდირების მონაცემებისა, რომლებიც შეიძლება გადაიცეს მობილური საკომუნიკაციო ქსელების მეშვეობით, რადარის ზონდირება სავარაუდოდ იქნება მომავალი უსადენო სისტემების განუყოფელი ნაწილი, როგორც კომუნიკაციის საშუალება, იგივე სპექტრისა და ტალღის ფორმის გამოყენებით. ეს ახალი შესაძლებლობები სანტიმეტრის დონის ლოკალიზაციის სიზუსტესთან

ერთად, ქსელს საშუალებას მისცემს, უკეთ გააცნობიეროს გარემო და მოიპოვოს სიტუაციური ცნობიერება (ანუ კომუნიკაციის კონტექსტის გაგება). მეორე მხრივ, ეს აჩენს უსაფრთხოების სხვა საკითხებს, რადგან თავად ზონდირების მონაცემები შეიძლება დაექვემდებაროს ხელყოფას თავდამსხმელებისგან, ამიტომ, მათი მთლიანობა უზრუნველყოფილი უნდა იყოს. შედეგად, ზონდირებისა და კომუნიკაციის სანდოობა, სავარაუდოდ, 6G სისტემების მუშაობის ძირითადი მაჩვენებელი იქნება.



ნახ. 2.1. სიმეტრიული გასაღებების დისტილაცია h_{AB} კოეფიციენტებიდან უსადენო მრავალგზიან არხებში, სადაც არხის ორმხრივობა გამოიყენება არხის კოჰერენტულობის დროს. პროცედურა მოიცავს სამ ფაზას, რომლებიც მოიხსენიება, როგორც უპირატესობის დისტილაცია, ინფორმაციის შეჯერება და კონფიდენციალურობის გაძლიერება

უსადენო პერიფერიაზე სწავლება და ბუნებრივი AI: ცენტრალიზებული ML, რომელიც მონაცემებს ცენტრალიზებულად, ღრუბელზე დაფუძნებული გამოთვლების გამოყენებით ამუშავებს, ექვემდებარება უსაფრთხოების კრიტიკულ გამოწვევებს (მაგალითად, მტყუნების ერთი წერტილი და მონაცემთა დაუცველობა ბექჰოლის დროს). უფრო მეტიც, ის შეიძლება არ იყოს შესაფერისი აპლიკაციებისთვის რეალურ დროში, მონაცემთა ცენტრალიზებული აგრეგაციისა და დამუშავების შედეგად მიღებული გამტარუნარიანობისა და შეყოვნების მოთხოვნების გამო. ამრიგად, დეცენტრალიზებული ML გადაწყვეტილებები სულ უფრო მნიშვნელოვანი ხდება (მაგალითად, ფედერირებული სწავლება, რომლის დროსაც მონაცემები ძირითადად, ადგილობრივად მუშავდება საბოლოო მომხმარებლის მოწყობილობებზე, სადაც ისინი გროვდება). მიუხედავად იმისა, რომ ასეთი განაწილებული ML გადაწყვეტილებები შეიძლება იყოს 6G მობილური პერიფერიული ქსელების გამაძლიერებელი ტექნოლოგიები, მათ ასევე შემოაქვთ დაუცველობა, როგორიცაა პირადი ინფორმაციის გაჟონვა ნასწავლი მოდელის პარამეტრების მეშვეობით, საბოლოო მომხმარებლის მავნე მოწყობილობების ზემოქმედება და თავდამსხმელების ტრენინგის მაგალითები.



ნახ.2.2. სრულგანზომილებიანი სხივის ფორმირება mMIMO-სთვის

6G-ის ეს მოსალოდნელი ფუნქციები გვაწვდის ახალ შესაძლებლობებს უსაფრთხოებისა და კონფიდენციალურობის ადრე აღწერილი გამოწვევების გადასაჭრელად, რაც საშუალებას იძლევა 6G ქსელების უსაფრთხოების არქიტექტურა აშენდეს ავტომატიზაციის გამოყენებით. მრავალმხრივი უსაფრთხოების პრინციპების გათვალისწინებით, სისტემამ ჩართული ობიექტების უსაფრთხოების მიზნები უნდა გაიგოს და შესაბამისად, უსაფრთხოების კონტროლის ადაპტირება მოახდინოს ახალი 6G ფუნქციებიდან მიღებული კონტექსტური ინფორმაციის საფუძველზე. ამ მიზნით, ჩვენ გვჭირდება სამშენებლო ბლოკების ნაკრები:

1. უსაფრთხოების რაოდენობრივი განსაზღვრა QoSec-ის ფარგლებში, ანუ სასურველი და რეალური „უსაფრთხოების დონის“ გამოხატვის უნარი.
2. კონტექსტური ცნობიერება უსადენო პერიფერიაზე ზონდირებისა და AI-ის გამოყენებით.

3. ახალი, ადაპტიური უსაფრთხოების კონტროლი, რომელიც მოიცავს PLS-ს.
4. ავტომატიზაცია ML/AI-ზე დაფუძნებული უსაფრთხოების ორკესტრატორის სახით.

ქვემოთ, ჩვენ უფრო დეტალურად განვიხილავთ ზოგიერთ ამ მნიშვნელოვან სამშენებლო ბლოკს.

QoS დეფინიციების მსგავსად (მაგალითად, ITU-T E.800), QoSec არის სერვისის მახასიათებლების ერთობლიობა, რომელიც გავლენას ახდენს მის უნარზე, დააკმაყოფილოს მომხმარებლის უსაფრთხოების განსაზღვრული და ნაგულისხმევი საჭიროებები. QoSec-ს შეუძლია უზრუნველყოს უსაფრთხოების სხვადასხვა გარანტია, სხვადასხვა გამოყენების შემთხვევისა და ერთმანეთთან დაკავშირებული ქსელის ნაწილების (network slices) უსაფრთხოების საჭიროებების საპასუხოდ, რაც აისახება დიფერენციალური სერვისების QoS პარადიგმაზე. QoSec-თან დაკავშირებული ცენტრალური ასპექტია იმის დადგენა, თუ როგორ გავხადოთ უსაფრთხოების დონე და მისი განხორციელება ადაპტიური: ანუ როგორ მოვახდინოთ სწორი QoSec-ის და კრიპტოგრაფიული სქემების სწორი კომბინაციის (დაშიფვრა, მთლიანობა, ავთენტიფიკაციის პრიმიტივები) ავტომატური იდენტიფიცირება; ასევე როგორ ჩავრთოთ ისინი მოქნილად უსაფრთხოების პროტოკოლებში.

ამრიგად, ადაპტაცია შეიძლება მოხდეს სხვადასხვა დონეზე: ფიქსირებული კრიპტოგრაფიული სიძლიერისთვის (მაგალითად, 256-ბიტიანი სიმეტრიული ბლოკური შიფრები კვანტური წინააღმდეგობის გათვალისწინებით) და ფიქსირებული თავდამსხმელის მოდელისთვის (მაგალითად, ნულოვანი სანდოობა, ანუ მინიმალური სანდოობის დაშვებები ყველა ჩართულ ობიექტთან დაკავშირებით), ჩვენ შეგვიძლია მოვახდინოთ იმ კონკრეტული კრიპტოგრაფიული ალგორითმებისა და პროტოკოლების ადაპტაცია, რომლებიც შემდგომ გამოიყენება. მეორე მხრივ, ჩვენ ასევე შეგვიძლია სასურველი კრიპტოგრაფიული სიძლიერის ან განხილული თავდამსხმელის მოდელის ადაპტირება კონტექსტურ ინფორმაციაზე დაყრდნობით. სამომავლო უსაფრთხოების პროტოკოლებში, სანდოობის სხვადასხვა დონე (მაგალითად, როგორც განსაზღვრულია NIST-ის მიერ SP800-53 Rev. 4-ში) გათვალისწინებულია უსაფრთხოების კონტროლის საბაზისო მოთხოვნების გამოყენებით. ასევე უნდა გავითვალისწინოთ, რომ ისინი შემუშავებულია რიგი ზოგადი დაშვებების საფუძველზე (მათ შორისაა გარემოს დაცვითი, ოპერატიული და ფუნქციონალური მოსაზრებები), რაც იწვევს უსაფრთხოების კონტექსტის გაცნობიერების საკითხის წამოწევას. მოგვიანებით, ჩვენ დეტალურად განვიხილავთ, თუ როგორ შეიძლება PLS-ის გამოყენება ადაპტიური უსაფრთხოების კონტროლის შესაქმნელად.

ტერაჰერცული სიხშირული სპექტრის გახსნა ახალი „შეგრძნების“ შესაძლებლობებს მისცემს 6G მოწყობილობებს, როგორიცაა მაღალი გარჩევადობის გამოსახულება და სიხშირის სპექტროსკოპია. წარმოიქმნება უნიკალური შესაძლებლობები კონტექსტური ცნობიერების მისაღწევად, როგორც ცენტრალიზებული, ისე პერიფერიული AI-ით ზონდირებული ინფორმაციის დამუშავების გზით; თავის მხრივ, კონტექსტური ცნობიერება არის სანდოობის ჩამოყალიბებისა და საიმედოობის პროგნოზირების გასაღები, ანუ QoSec შეიძლება განპირობებული იყოს კონტექსტური ცნობიერებით. უსაფრთხოების კონტროლში კონტექსტური ცნობიერების ჩართვა ნიშნავს AI-ის დახმარებით პასუხის გაცემას შემდეგ ღია კითხვებზე:

როგორ შეიძლება საფრთხის დონის ექსტრაპოლაცია კონტექსტიდან: ფიზიკური (PHY) ფენის შემავალი მონაცემები, განსაკუთრებით ინფორმაციის აღქმის სახით, მათ შორის კვანძის მდებარეობა, კომუნიკაციის დრო, გარემო ტემპერატურა და ა. შ. შეიცავს მნიშვნელოვან კონტექსტურ ინფორმაციას, რომელიც პირდაპირ კავშირშია სემანტიკასთან. ჩვენ შეგვიძლია წარმოვიდგინოთ AI-ის მულტიმოდალური შერწყმა ზონდირების ინფორმაციის მისაღებად, რათა საფრთხის დონის გაუმჯობესებული შეფასება მივიღოთ. ძალიან მომთხოვნ სცენარებში, როგორიცაა მოწესრიგებულად გადაადგილებად ავტოკოლონასთან ურთიერთობა, ეს მიდგომა შეიძლება დაეხმაროს სიცოცხლისუნარიანი მარშრუტის შექმნას ანო-

მალიების აღმოჩენის გადაწყვეტილებების შემუშავებაში უაღრესად დინამიკური და ერთი შეხედვით, ქაოტური ქსელებისთვის.

როგორ გამოიყენება კონტექსტი საჭირო უსაფრთხოების დონის დასადგენად: ჩვენ უნდა გადავდგათ ნაბიჯები ახალი მეტრიკის განსაზღვრისკენ, რომელიც აღწერს გაცვლილი კონკრეტული მონაცემების კრიტიკულობას და, გარდა ამისა, განსაზღვრავს, რამდენად ღირებულია ისინი თავდამსხმელის თვალსაზრისით. ეს შეიძლება განხილული იქნეს QoS-ში პრიორიტეტის დონის განსაზღვრის ანალოგიურად.

როგორ ემთხვევა უსაფრთხოების დონეები უსაფრთხოების სქემებს: როდესაც უსაფრთხოების დონე განისაზღვრება კომუნიკაციის კონტექსტიდან გამომდინარე, ბუნებრივად ჩნდება კითხვა, როგორ ავსახოთ ეს ალგორითმებისა და უსაფრთხოების სქემების რეალურ კომპლექტზე. არსებობს ორი მიდგომა, რომელთა გამოყენება შესაძლებელია ერთობლივად:

- კრიპტოგრაფიაზე დაფუძნებული მიდგომები, რომლებშიც კრიპტოსისტემების სიძლიერე, უხეშად რომ ვთქვათ, დაკავშირებულია გასაღებების სიგრძესთან (სწორი გარდაქმნების გათვალისწინების შემდეგ).
- PLS მიდგომები, რომლებშიც უსადენო არხი და HW გამოიყენება უნიკალურობისთვის (ავთენტიფიკაციისთვის) და/ან ენტროპიის წყაროდ კონფიდენციალურობის მიზნებისთვის (მაგალითად, SKG-სთვის).

შემდეგ პარაგრაფში ჩვენ შევისწავლით PLS-ის პოტენციურ გამოყენებას 6G-ში და განვიხილავთ, თუ როგორ არის PLS არსებითად ადაპტირებული და როგორ შეიძლება იყოს ის ჩართული კონტექსტური ცნობიერებით.

2.4. QoSec ადაპტიური უსაფრთხოების კონტროლი: ფიზიკური ფენის უსაფრთხოების როლი 6G-ში

წარსულში, PLS იყო შესწავლილი და მოხსენიებული, როგორც ქსელების გათავისუფლების შესაძლო გზა კლასიკურ სირთულეზე დაფუძნებული უსაფრთხოების მიდგომებისგან. PLS დაფუძნებულია წინაპირობაზე, რომ ჩვენ შეგვიძლია გავაუმჯობესოთ უსაფრთხოების ზოგიერთი ძირითადი ფუნქცია, ვიყენებთ რა საკომუნიკაციო რადიოარხს და HW-ის, როგორც უნიკალურობის ან ენტროპიის წყაროებს.

ჩვეულებრივ, PLS-ის ეს ასპექტი განიხილება ლიტერატურაში, საიდუმლოების გამტარუნარიანობის და SKG გამტარუნარიანობის კონცეფციასთან დაკავშირებით. ამ სტრუქტურაში, PLS იყენებს რადიოარხის ფიზიკურ თვისებებს, კერძოდ, დიფუზიას, სუპერპოზიციას და ორმხრივობას, რათა შექმნას შესაძლებლობები უსაფრთხო მონაცემთა გადაცემისთვის არხში მომსმენების თანდასწრებით. ამ თვისებების გამოყენება შესაძლებელია სხვადასხვა გზით, მათ შორის, ლეგიტიმურ მომხმარებლებსა (LU) და მომსმენებს შორის დამოუკიდებელი ფედინგის უპირატესობის გამოყენებით, მრავალანტენიანი სისტემის ან სარელეო გადაცემის გამოყენებით და ხელოვნური ხმაურის ინექციით თავისუფლების უსაფრთხო ხარისხის შესაქმნელად.

ა. ვაინერის მიერ 1975 წელს შემუშავებულ ცნობილ მოსმენის არხის მოდელში, მოწინააღმდეგე ლინკი დეგრადირებულია მთავარ ლინკთან მიმართებაში, ანუ ლეგიტიმური მომხმარებლები არ აზიარებენ საიდუმლოს, მაგრამ აქვთ ლინკის ხარისხის უპირატესობა. როდესაც ამის დასაბუთება შესაძლებელია, ნაჩვენებია მოსმენების კოდების არსებობა, რომლებსაც შეუძლიათ ასიმპტომურად უზრუნველყონ როგორც ლეგიტიმური მიმღების მიერ კონფიდენციალური შეტყობინების მიღების სანდოობა, ასევე

ინფორმაციის უმნიშვნელო გაჟონვა მომსმენისთვის. გარდა ამისა, ქსელის/სისტემის პარამეტრების კორექტირებით მიიღწევა საიდუმლოების დარღვევის სხვადასხვა ალბათობა, რომელიც პოტენციურად შეესაბამება QoSec-ის სხვადასხვა დონეს. ჩვენ განვიხილავთ გამოყენების შემთხვევების ძირითად იდეებს, როდესაც მოსმენის არხი გამოიყენება ჰიბრიდული PLS კრიპტოსისტემების სიმეტრიული საიდუმლო გასაღებების უსაფრთხოდ გადასაცემად. ამ შემთხვევაში, საიდუმლოების ძალიან დაბალი დონე შეიძლება მიმართული იყოს 256-ბიტიან ერთ გასაღებზე და შეიძლება გამოყენებულ იქნეს გიგაბაიტამდე მონაცემთა დაშიფვრისთვის; მაგალითად, როდესაც მოსმენების კოდირება გამოიყენება თანამედროვე შიფრებთან ერთად, როგორიცაა დაშიფვრის მოწინავე ალგორითმი (AES) გალუას მრიცხველის რეჟიმში (GCM), შეიძლება საკმარისი იყოს საიდუმლოების ხარისხი, 10^{-7} რიგის შესაბამისად. ამ დაშვების მიხედვით, ჩვენ ვაჩვენებთ სისტემის დიზაინის პარამეტრებს, რათა მივაღწიოთ საიდუმლოების პოზიტიურ მაჩვენებლებს ორ სცენარში: (ა) ცხრილში 2.1 ჩვენ ვაფასებთ ანტენების მინიმალურ რაოდენობას საბაზო სადგურზე მრავალშესასვლელიანი და ერთგამოსასვლელიანი (MISO) არხებისთვის და (ბ) ცხრილში 2.2, მოსმენის მაქსიმალური სიმკვრივე შეფასებულია უპილოტო საფრენი აპარატების (UAV) ქსელებისთვის.

	$P_{so} = 10^{-1}$	$P_{so} = 10^{-3}$	$P_{so} = 10^{-5}$	$P_{so} = 10^{-10}$
$\alpha_e/\alpha_u = 1/4$	1	3	7	21
$\alpha_e/\alpha_u = 1/2$	2	10	37	698
$\alpha_e/\alpha_u = 1$	9	952	—	—

ცხრილი 2.1. ანტენების მინიმალური რაოდენობა N_t , რომელიც საჭიროა MISO-ს დაუნლინკის ქსელის BS-ზე, მომსმენის ერთი ანტენის თანდასწრებით, სამიზნის საიდუმლოების დარღვევის P_{so} ალბათობისთვის

	$P_{so} = 10^{-1}$	$P_{so} = 10^{-3}$	$P_{so} = 10^{-5}$	$P_{so} = 10^{-10}$
$\lambda_u = 10^{-3}$	1	10^{-1}	10^{-3}	10^{-8}
$\lambda_u = 10^{-2}$	1	10^{-2}	10^{-4}	10^{-9}

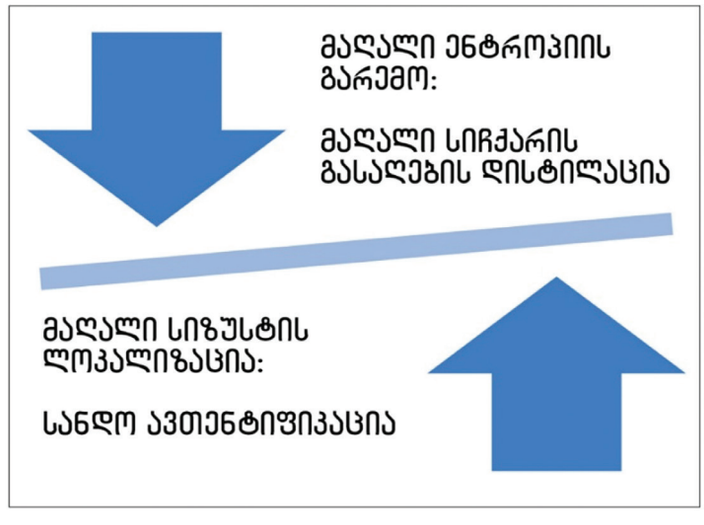
ცხრილი 2.2. მოსმენის მაქსიმალური სიმკვრივე λ_e უპილოტო საფრენი აპარატების (UAV) ქსელში სამიზნის საიდუმლოების დარღვევის P_{so} ალბათობის მისაღწევად. λ_u აღნიშნავს ლეგიტიმური კვანძების სიმკვრივეს, ხოლო UAV იმყოფება 10 მ სიმაღლეზე

ცხრილში 2.1 შესამჩნევია მოწინააღმდეგის ლინკის ლეგიტიმურ ლინკთან შედარებითი ხარისხის კრიტიკული როლი. აღნიშნული წარმოდგენილია ფართომასშტაბიანი ფედინგის კოეფიციენტების თანაფარდობით, რომელიც შესაბამისად აღინიშნება, როგორც α_e და α_u. როდესაც ლეგიტიმური მომხმარებელი ბევრად ახლოსაა საბაზო სადგურთან, ვიდრე მოწინააღმდეგე, საიდუმლოების დარღვევის ალბათობა 10^{-10}-მდე შეიძლება მიღწეული იყოს მხოლოდ 21 ანტენის გამოყენებით. მეორე მხრივ, UAV კომუნიკაციებში პირდაპირი ხედვის ხაზის არსებობის გამო, მოსმენის მაქსიმალური სიმკვრივე საიდუმლოების დარღვევის იმავე ალბათობისთვის არის $\lambda_e = 10^{-8}$, როდესაც ლეგიტიმური კვანძების სიმკვრივეა $\lambda_u = 10^{-3}$ და UAV მიწიდან 10 მ სიმაღლეზეა. მხოლოდ საიდუმლოების დარღვევის ალბათობის

გაზრდით (ანუ სამიზნე QoSec დონის შემცირებით) შეიძლება გაიზარდოს მოსმენის მაქსიმალური სიმკვრივე. ეს ორი მაგალითი ცხადყოფს, რომ კონტექსტის გაცნობიერება აუცილებელია PLS-ის სათანადო გამოყენებისთვის: წვდომის წერტილთან (AP) სიახლოვე გადამწყვეტია MISO პარამეტრებში; UAV-ის მაგალითში კვანძების სიმკვრივე მნიშვნელოვან როლს ასრულებს. ეს ორი მაგალითი ასევე აჩვენებს, რომ ამ კონტექსტში PLS შეიძლება გამოყენებულ იქნეს ქვეჯგუფის QoSec დონეების პოტენციურად მისაღწევად, რომელიც დაკავშირებულია საიდუმლოების დარღვევის ალბათობებთან.

6G-ში მოსმენის კოდების გამოყენების კიდევ ერთი მნიშვნელოვანი შემთხვევა წარმოიქმნება დაბალი შეყოვნების სისტემებთან მიმართებაში, რომლებიც მოკლე პაკეტებს იყენებენ. სასრული ბლოკის სიგრძის მოსმენის არხში შეუძლებელია ინფორმაციის ნულოვანი გაჟონვის მიღწევა, როგორც ამას ადგილი აქვს ასიმპტოტური რეჟიმისათვის. აქ მცირე მნიშვნელობის δ სიდიდეა შემოტანილი, როგორც გარანტირებული ზედა ზღვარი ინფორმაციის გაჟონვის თვალსაზრისით. ჩვენ ვვარაუდობთ, რომ დაბალი ფასის მქონე IoT ქსელებში, რომლებშიც შეიძლება QoSec უსაფრთხოების პოტენციურად დაბალი დონე იყოს მისაღები, გაჟონვის მაქსიმალური სიჩქარის δ დაშვება შესაძლოა იყოს კონფიდენციალურობის გარანტიების უზრუნველყოფის გზა.

გარდა ამისა, როგორც უკვე აღვნიშნეთ, PLS-ის გამოყენება ისარგებლებს ძალიან ვიწრო სხივებით, რომელიც სავარაუდოდ, ხელმისაწვდომი იქნება 6G-ში, რადგან ისინი ძალიან გაართულებენ მოსმენას თავდამსხმელებისთვის, რომლებიც არ არიან განლაგებული სხივის მიმართულებით და იგივე სამართლიანი იქნება VLC-ის შემთხვევაშიც. გარდა ამისა, სიხშირის გატარების ფართო ზოლს შეუძლია უზრუნველყოს საკმარისი ენტროპია, მაღალსიჩქარიანი საიდუმლო გასაღებების შესაქმნელად. SKG სქემები უსადენო კოეფიციენტებიდან, ალბათ, ყველაზე მომწიფებულია ყველა PLS ტექნოლოგიას შორის. თუმცა, კონტექსტის გაცნობიერება გადამწყვეტია SKG-ის 6G სისტემებში ჩართვისთვის. კერძოდ, როდესაც იცვლება პირდაპირი ხედვის ხაზის პირობები და არხის ხარისხი, აშკარაა ურთიერთკომპრომისი მაღალი სიზუსტის ლოკალიზაციისთვის უსადენო ფედინგის გამოყენებას (რაც მთავარია, შემდგომ განხილული PLS ავთენტიფიკაციისთვის) და ენტროპიის დისტილაციის საშუალებებს (გასაღებების შეთანხმების, კონფიდენციალურობისა და მთლიანობის უზრუნველყოფის სქემებისთვის) შორის, როგორც ეს ნაჩვენებია ნახ. 2.3-ზე. ამ უნიკალური პარამეტრის გამოყენება შესაძლებელია მხოლოდ უსადენო არხისა და ზოგადად, კონტექსტის მოწინავე მონიტორინგით, რაც კიდევ ერთხელ ადასტურებს, რომ კონტექსტის გაცნობიერება ნამდვილად გამაძლიერებელია PLS-სთვის.



ნახ. 2.3. უსადენო არხს შეუძლია იმოქმედოს, როგორც ენტროპიის წყარო ან როგორც ავთენტიფიკაციისთვის მაღალი სიზუსტის ლოკალიზაციისა და პოზიციონირების წყარო

მომხმარებლის ავთენტიფიკაციასთან დაკავშირებით, ჩვენ შეგვიძლია დავიხმაროთ PHY ფენა RF თითის ანაბეჭდის და მაღალი სიზუსტის ლოკალიზაციის გამოყენებით, როგორც „რბილი“ ავთენტიფიკაციის ფაქტორები. აღსანიშნავია, რომ მომავალი ქსელების მრავალი ახალი მახასიათებელი, როგორიცაა დაბალი შეყოვნების კონტროლის მარყუჟები, სენსორების შერწყმა და ერთდროული ლოკალიზაცია, კარტოგრაფია, დასჭირდება მხოლოდ ადგილობრივ კომუნიკაციას, რომელიც არ მოიცავს ძირითად ქსელს. ის შეიძლება გახდეს უფრო უსაფრთხო და მოქნილი PLS-ის გამოყენებით, რაც ქსელზე დაფუძნებული ცენტრალიზებული უსაფრთხოების საჭიროებას ამცირებს. ამ კონტექსტში, ML-ით მხარდაჭერილი PLS შეიძლება გამოყენებულ იქნეს ინტელექტუალური PHY ავთენტიფიკაციისთვის დინამიკურ და რთულ 6G გარემოში, როგორიცაა IoT ქსელები. ML მეთოდების ბაზაზე კომპლექსური მახასიათებლების სტატისტიკის შესწავლისა და აღბეჭდვის შესაძლებლობის წყალობით, ჩვენ შეგვიძლია მივაღწიოთ დაბალფასიან, უწყვეტ, მაღალი საიმედოობის მქონე, მოდელისგან დამოუკიდებელ და კონტექსტის მიხედვით გაცნობიერებულ ავთენტიფიკაციას (მაგალითად, ლოკალიზაციის და RF თითის ანაბეჭდის გამოყენებით). ასეთი ავთენტიფიკაციის მექანიზმების საიმედოობის გასაუმჯობესებლად საჭიროა დაკვირვებაში მყოფი და შეფასებული ატრიბუტების სანდოობის მონიტორინგი, კონტექსტის გათვალისწინებით.

დაბოლოს, მოწყობილობის ავთენტიფიკაციის კუთხით, შემდგომში შესაძლებელია „ტექნიკური თითის ანაბეჭდების“ გამოყენება ფიზიკური არაკლონირებადი ფუნქციების (PUF) სახით, როგორც ავთენტიფიკაციის ფაქტორი მრავალფაქტორიანი ავთენტიფიკაციის პროტოკოლებში. PUF-ები ეყრდნობა ვაინერ-ზივის შეთანხმების მიდგომების გამოყენებას, რათა უზრუნველყოს აპარატურული თითის ანაბეჭდის გაზომვადი, ხელახალი გამოყენების შესაძლებლობა. სხვადასხვა PLS ტექნოლოგიის კომბინაციით, ჰიბრიდული PLS კრიპტოსისტემები შეიძლება შემუშავდეს ნულოვანი ორმხრივი მგზავრობის დროის პროტოკოლების და/ან ავთენტიფიკაციის დაშიფვრის იდეებზე, რაც გვთავაზობს დამატებით ინსტრუმენტებს PHY-ში სწრაფი ავთენტიფიკაციის სქემების შესაქმნელად, ავთენტიფიკაციის მრავალი ფაქტორის პოტენციური გამოყენებით.

2.5. დისკუსია და შემოთავაზებული გზამკვლევი რუკა

ფართო სურათის გათვალისწინებით, 6G-სკენ მიმავალ გზაზე, ჩნდება ახალი უსაფრთხოების გამოწვევები და შესაძლებლობები. გამოწვევებს შორის აღსანიშნავია საკითხები, რომლებიც დაკავშირებულია დაუცველობასთან კვანძის ქსელში შესვლის საწყის ფაზებში (5G უსაფრთხოების პროტოკოლების ამოქმედებამდე), დაბალი ფასის და ჰეტეროგენული IoT მოწყობილობების უზარმაზარ რაოდენობასთან, ქვემილიწამიანი დაყოვნების შეზღუდვებთან, IoT-ის გამოყენების კრიტიკულ შემთხვევებთან და სხვა. ყოველივე აღნიშნული მნიშვნელოვანია პოსტკვანტური უსაფრთხოების გარანტიების შეთავაზებისა და კონფიდენციალურობის საკითხების განხილვისას. მეორე მხრივ, მოსალოდნელია, რომ 6G იქნება უსადენო ქსელების პირველი თაობა, რომელიც შემოგვთავაზებს პერიფერიულ და მოწყობილობის დონეზე ინტელექტს, ახალი ზონდირების შესაძლებლობების და ML-ის ფართო გამოყენებით.

6G უსაფრთხოების პროტოკოლებში კონტექსტური ცნობიერების ჩართვამ შეიძლება ხელი შეუწყოს ახალი „გამრღვევი“ ტექნოლოგიების დანერგვას, უსაფრთხოებასთან დაკავშირებული საფრთხის დონის ონლაინშეფასების საფუძველზე მოქნილი და ადაპტიური გარანტიების უზრუნველსაყოფად. სწორედ ამ კონტექსტშია შესაძლებელი PLS ტექნოლოგიების რეალურად გამოყენება; PLS შეიძლება განხო-

რციელდეს მხოლოდ 6G-ში საკომუნიკაციო გარემოსა და საკომუნიკაციო საშუალების ყოველმხრივი შესწავლით და საიმედო მონიტორინგით. ისეთ აპლიკაციებში, როგორიცაა IoT, PLS ხდება ძალიან კონკურენტუნარიანი კანდიდატი, რომელიც გამოიყენება კონტექსტით გაცნობიერებული, მოქნილი და ადაპტირებული უსაფრთხოების კონტროლისთვის, როგორც ავთენტიფიკაციის, ასევე კონფიდენციალურობის სქემებისთვის. მიუხედავად იმისა, რომ PLS შესაძლოა, სულ მცირე, უახლოეს მომავალში არ იყოს ჩართული ნულოვანი სანდოობის უსაფრთხოების პროტოკოლებში, ის იძლევა სიცოცხლისუნარიან ალტერნატივას მასობრივი და ულტრა დაბალი შეყოვნების ქსელების უსაფრთხოების გარანტიებით, როგორც კონკურენტუნარიანი კანდიდატი განვითარებადი QoSec მიდგომებისთვის, რომლებიც მოიცავს ქსელის სტეკის ყველა ფენას.

PLS გვთავაზობს მნიშვნელოვან უპირატესობებს. პირველი, ის თავისებურად ადაპტირებადია; სამიზნე უსაფრთხოების ან საიდუმლო გასაღების სიჩქარის კორექტირებით, უსაფრთხოების დარღვევის შესაბამისი ალბათობა შეიძლება მორგებული იყოს შესაბამის გარემოზე, რაც უზრუნველყოფს მოქნილ სტრუქტურას უსაფრთხოების ადაპტირებული კონტროლისთვის. გარდა ამისა, PLS-ს შეუძლია უზრუნველყოს ინფორმაციულ-თეორიული უსაფრთხოების გარანტიები მსუბუქი მექანიზმების გამოყენებით (მაგალითად, პოლარული ან დაბალი სიმკვრივის ლუწობის შემმოწმებელი (LDPC) კოდერების გამოყენებით) გამოთვლითი კუთხით ძვირად ღირებული კრიპტოგრაფიული სქემებისგან განსხვავებით. ამრიგად, ასეთი მიდგომები შესაფერისია დაბალი სირთულის IoT მოწყობილობებისთვის და ქსელებისთვის მსუბუქი ინფრასტრუქტურით ან მის გარეშე, როგორც დამოუკიდებელი უსაფრთხოების საუკეთესო მექანიზმები ან როგორც უფრო ტრადიციული მეთოდების დანამატი.

ზემოთ განხილული ზოგიერთი პუნქტის საილუსტრაციოდ, ცხრილში 2.3 ჩვენ წარმოვადგენთ გზამკვლევ რუკას, თუ როგორ უნდა გადავჭრათ ადრე ჩამოთვლილი უსაფრთხოების გამოწვევები და როგორ ჯდება PLS ამ სურათში. გვინდა ხაზგასმით აღვნიშნოთ, რომ წარმოდგენილი იდეები ჯერ კიდევ მხოლოდ თავსატეხის ნაწილია და ინტეგრირებული უნდა იყოს ბევრად უფრო ჰოლისტიკურ მიდგომაში, რომელიც ტექნიკურ საშუალებებთან ერთად დამატებით უნდა მოიცავდეს ორგანიზაციულ, მარეგულირებელ, ეკონომიკურ და სტანდარტიზაციის ასპექტებს.

2.6. მეორე თავის დასკვნა

უდავოდ, 5G უსაფრთხოების გაუმჯობესებები წარმოადგენს გარკვეულ ნახტომს LTE-სთან მიმართებაში. თუმცა, როდესაც აპლიკაციის სცენარების სირთულე იზრდება ახალი გამოყენების შემთხვევების, განსაკუთრებით URLLC-ის და mMTC-ის დანერგვით, წარმოიქმნება ახალი უსაფრთხოების გამოწვევები, რომელთა მოგვარება შეიძლება პრობლემატური იყოს სირთულეზე დაფუძნებული კლასიკური კრიპტოგრაფიული გადაწყვეტილებების სტანდარტული პარადიგმის გამოყენებით. ამავდროულად, უფრო გრძელ, 10-წლიან ჰორიზონტზე გაჩნდება უსაფრთხოების ახალი კონცეფციები, რომლებიც დაფუძნებულია „სანდოობის მოდელებზე“ და რისკზე დაფუძნებული ადაპტირებულ პირადობის მენეჯმენტსა და წვდომის კონტროლზე, რაც დიდწილად იქნება შესაძლებელი AI-ის საშუალებით. QoSec-ის მოქნილობის უზრუნველსაყოფად, გათვალისწინებულია უსაფრთხოების კონტროლის შემუშავება და ინტეგრაცია საკომუნიკაციო სისტემის ყველა ფენის მიხედვით.

ამ სტრუქტურაში, PLS განიხილება, როგორც ქსელების გათავისუფლების შესაძლო გზა კლასიკურ სირთულეზე დაფუძნებული უსაფრთხოების მიდგომებისგან. ავთენტიფიკაციასთან დაკავშირებით, PUF-ები, უსადენო თითის ანაბეჭდები და ლოკალიზაცია, უფრო კლასიკურ მიდგომებთან ერთად,

ასევე აუმჯობესებენ ავთენტიფიკაციას და გასაღების შეთანხმებას რთულ და მოთხოვნად სცენარებში. პარალელურად, ტერაჰერცული კომუნიკაციები დაეყრდნობა მაღალი მიმართულობის მქონე სხივების შექმნას, რაც პოტენციურად უზრუნველყოფს კონკრეტულ სცენარს მოსმენის არხისთვის. გარდა ამისა, 6G-ში უფრო მაღალი სიხშირული დიაპაზონის გახსნით, სიხშირის დომენში ენტროპიის გამოყენების შესაძლებლობა შეიძლება ჩადებულ იქნეს SKG პროტოკოლებში. როგორც ზოგადი მიმართულება, კონტექსტური ცნობიერება, რომელიც გამოყენებული იქნება 6G-ში მოსალოდნელი ზონდირების და AI-ის გაუმჯობესებული შესაძლებლობებით, საშუალებას მოგვცემს დავნერგოთ „გამრღვევი“ ინსტრუმენტები ადაპტიური, QoSec-ზე დაფუძნებული უსაფრთხოების გარანტიების უზრუნველსაყოფად, რომლებიც მორგებული იქნება კომუნიკაციის კონტექსტზე PLS-ის უსაფრთხოების კონტროლის მეშვეობით.

უსაფრთხოების გამოწვევა/სცენარი	რეკომენდებული ტექნიკა (*-ით აღნიშნულია PLS/PHY გადაწყვეტილებები)
ყალბი საბაზო სადგურის თავდასხმები	* ინტელექტუალური PHY ავთენტიფიკაცია RF თითის ანაბეჭდის გამოყენებით და BS-ის ლოკალიზაცია UE-დან (შებრუნებული ლოკალიზაცია) * წინასწარ გაზიარებული გასაღებები დაყენებულია/განაწილებულია SKG-სთან
დაბალი შეყოვნების კომუნიკაციები	* სწრაფი ავთენტიფიკაცია PUF-ების და RF თითის ანაბეჭდის გამოყენებით, როგორც აღრეული ავთენტიფიკაციის ფაქტორები * მოკლე პაკეტების საიდუმლო კოდირება * მოკლე ბლოკის სლეპიან-ვულფის და ვაინერ-ზივის შეჯერების დეკოდერები (SKG და PUF-ებისთვის)
თავდასხმების ჩახშობა mMIMO-ში – RF მდგრადობა	* სპექტრის ზონდირება, არხის დიაგრამის შემუშავება, არხის შესწავლა * გაუმჯობესებული მოდულაცია და კოდირება * შეჭრის გამოვლენა PHY-ში * ფარული კომუნიკაციები/გამოვლენის დაბალი ალბათობა
კონფიდენციალურობა	– კონტექსტით გაცნობიერებული ფსევდონიმი, ნაწილობრივი იდენტობა – კონტექსტით გაცნობიერებული მთლიანობა დარღვევების აღმოსაჩენად და შესამსუბუქებლად – კონტექსტით გაცნობიერებული შესაბამისობა და განაწილება
პოსტკვანტური მდგრადობა	* PLS არის ინფორმაციულ-თეორიული უსაფრთხოება * გრძელი სიმეტრიული დაშიფვრის გასაღებები არხზე დაფუძნებული გასაღების გენერირების გამოყენებით * ჰიბრიდული კრიპტო-PLS სქემები
იაფი IoT მოწყობილობები	* მსუბუქი PLS, საიდუმლო კოდირება, SKG, PUF-ები და ა.შ. იაფი/დაბალი უსაფრთხოების IoT მოწყობილობების ინფორმირებულობა შესაბამისი იზოლაციისთვის ქსელის განკუთვნილ ნაწილში
IoT მოწყობილობების დიდი რაოდენობა	– კონტექსტური გაგება, რომ ავტომატურად შეარჩიოს შესაბამისი QoSec – უსაფრთხოების კონტროლის ადაპტირებული და ავტომატური ელემენტები, რომლებიც აგვაცილებენ პრობლემას, რომ ხელით დავაკონფიგურიროთ და დავაკვირდეთ ყველა IoT მოწყობილობას · PLS, როგორც მასშტაბირებადი ტექნოლოგია გასაღების მართვისა და განაწილებისათვის · PLS, როგორც ადაპტიური უსაფრთხოების სქემა
გრძელვადიანი IoT უსაფრთხოება	– დროთა განმავლობაში QoSec-ის და სანდოობის შემცირების გაცნობიერება – უსაფრთხოების ზოგადი კონტროლისა და პოლიტიკის ავტომატური დაშვება – კონტექსტით გაცნობიერებული წვდომის კონტროლი, მაგალითად, არასანდო მოწყობილობების ქსელიდან გამორიცხვა ან (წვდომის) უფლებების შემცირება

ცხრილი 2.3. გადაწყვეტილებების გზამკვლევი რუკა 5G/6G უსაფრთხოების გამოწვევებისთვის

თავი 3. მოძრავი სამიზნეების დაცვა და მისი ინტეგრირება B5G სისტემების უსაფრთხოების არქიტექტურაში

3.1. შესავალი

5G ქსელები შექმნილია მრავალი სერვისის უზრუნველსაყოფად, როგორც ყოვლისმომცველი მამოძრავებელი ძალა დაკავშირებული ციფრული აპლიკაციებისთვის ნებისმიერ დროს და ნებისმიერ ადგილას. ისინი კონცეპტუალიზებულია, როგორც მრავალმომხმარებლიანი და მრავალდომენიანი ქსელები ვირტუალიზებული სერვისებით/რესურსებით, რომლებიც მუშაობს მოქნილ, SW-ით განსაზღვრულ ქსელზე. ეს სერვისები, დაწყებული გასართობი აქტივობებიდან, როგორიცაა ვიდეონაკადი, დამთავრებული მისიისთვის კრიტიკულად მნიშვნელოვანი გამოყენებებით, ასევე აპლიკაციებით, როგორიცაა ინტელექტუალური ქსელები ან IIoT, უნდა ოპერირებდნენ მასშტაბირებადი, ეკონომიური და ელასტიკური გზით. B5G ან 6G სისტემები მკვეთრად გააფართოებს ქსელის შესაძლებლობებს ამ დაპირების მიღმა და მოახდენს სერვისების რევოლუციური კომპლექტის რეალიზაციას უპრეცედენტოდ მაღალი ხარისხისა და საიმედოობის დონეებით, როგორიცაა შემდგომი გაუმჯობესებული მობილური ფართოზოლოვანი ქსელი (FeMBB), გაუმჯობესებული (ულტრა) საიმედო დაბალი შეყოვნების მქონე კომუნიკაცია (ERLLC/eURLLC) და ულტრა მასობრივი მანქანური ტიპის კომუნიკაცია (umMTC). ისინი გათვალისწინებულია 1 ტბტ/წმ მონაცემთა გადაცემის პიკური სიჩქარის, 1 ტბ/წმ/მ^2 ფართობის ერთეულზე ტრაფიკის გამტარუნარიანობის და მიკროწამის დონის შეყოვნების მხარდაჭერად. ნავარაუდევია, რომ ისინი განლაგდება 2030-იან წლებში და ფართოდ გაუხსნის გზას ტრაფიკის გაფართოებულ მოთხოვნებს უფრო მოქნილი, მონაცემებისთვის ტევადი და ტაქტილური აპლიკაციებისთვის, როგორიცაა ჰოლოგრაფიული კომუნიკაციები, ყოვლისმომცველი ვირტუალური რეალობის (VR) და XR-ის გამოყენებები, ჭკვიანი მასობრივი ავტონომიური სისტემები, როგორიცაა: დრონები, მიწოდების სერვისი, სამგანზომილებიანი ქსელი და სრულად ავტომატიზებული ქსელის მართვა.

თუმცა, ამ 6G ეკოსისტემის გაზრდილი სირთულე გამოიწვევს უფრო დიდი თავდასხმის ზედაპირის არსებობას, რაც უკვე აქტუალური საკითხია, თუნდაც მიმდინარე 5G განვითარებისთვის. ამასთან დაკავშირებით, მავნე აგენტს შეუძლია შეასრულოს სხვადასხვა თავდასხმა, როგორიცაა სერვისზე განაწილებული უარის თქმა (DDoS), გაყალბება და MitM. მას ასევე შეუძლია თავდასხმა ქსელის შიგნიდანაც კი, ვინაიდან ერთმა კომპრომეტირებულმა მოწყობილობამ შეიძლება გამოიწვიოს უსაფრთხოების ფართოდ გავრცელებული ინციდენტები, როგორც ეს ბოლოდროინდელი IoT ბოტნეტებიდან ჩანს. ასეთ შემთხვევაში სერიოზულ გამოწვევას წარმოადგენს თავდასხმების პრევენცია და შემსუბუქება ფართომასშტაბიან 5G სერვისებში და პერსპექტიული 5G ინფრასტრუქტურის მიღმა (მაგალითად, 6G-სთვის). აუცილებელი ხდება ავტომატიზებული სისტემის არსებობა, რომელიც მონიტორინგს უწევს, პროაქტიულად იცავს, აღმოაჩენს და ადაპტირებულად ამცირებს საფრთხეებს, თავდასხმის ზედაპირის შეცვლით, ოპტიმალური და დინამიკური გადაწყვეტილებების შესრულებით და ქსელის ფუნქციონირების მრავალი ფაქტორის გათვალისწინებით.

MTD არის პერსპექტიული დაცვის პარადიგმა, რომელიც შეიძლება გამოყენებულ იქნეს ამ სასიცოცხლო გამოწვევების გადასაჭრელად. ამ კონცეფციის პრინციპია ქსელისა და სერვისების კონფიგურაციისა და ტოპოლოგიის მუდმივად შეცვლა, რაც მას დინამიკურ გარემოდ აქცევს. ეს მკვეთრად ზღუდავს მავნე მომხმარებელთა სამოქმედო სივრცეს დროისა და სივრცის განზომილებებში, რადგან დაზვერვითი თავდასხმებით და თითის ანაბეჭდზე დაფუძნებული თავდასხმებით შეგროვებული

ინფორმაცია ხდება მოძველებული, შეუსაბამო ქსელის სეგმენტებისთვის და გამოუსადეგარი თავდასხმის სტრატეგიებისთვის. იდეალურ შემთხვევაში, MTD პროაქტიულად აღმოფხვრის ასიმეტრიულ უპირატესობას, რომელიც ჩვეულებრივ აქვს თავდამსხმელებს ქსელის უსაფრთხოების მენეჯერთან მიმართებაში – ამ უკანასკნელმა წინასწარ არ იცის, ვინ არის თავდამსხმელი ან რა შესაძლებლობები აქვს, განსხვავებით პირველისგან, რომელიც ჩვეულებრივ აყალიბებს და შემდეგ დეტალურად ამუშავებს თავდასხმის სტრატეგიებს და მისი მეთოდები განკუთვნილია კონკრეტული მიზნის მისაღწევად. ახალ ძირითადი მახასიათებლების ინდიკატორებს (KPI), რომლებიც გათვალისწინებულია B5G და 6G სისტემებისთვის, გადამწყვეტი მნიშვნელობა აქვს MTD-ის პრაქტიკულობისთვის ამ ყოვლისმომცველ პერსპექტიულ სისტემებში. მიუხედავად ამისა, MTD-ის, როგორც თავდაცვის ელემენტის მიღება, ქმნის ოპტიმიზაციისა და კონტროლის პრობლემას უსაფრთხოების მენეჯმენტისთვის. ამ მიზნით, AI-ის და ML-ის მოწინავე მეთოდების გამოყენება გადამწყვეტია MTD სტრატეგიების ოპტიმიზაციისთვის, პრობლემების პრევენციის (პროაქტიული სქემები) და შემსუბუქების (რეაქტიული სქემები) კუთხით, რაც ხელს უწყობს დაცვის მიმართ ავტონომიურ მიდგომას და უზრუნველყოფს დაცული სერვისების ხელმისაწვდომობას.

უსაფრთხოების მზარდი გამოწვევებისა და უსაფრთხოების პროაქტიული, ავტონომიური სქემების საჭიროების გათვალისწინებით, AI/ML-თან ინტეგრირებული MTD განსაკუთრებით საჭიროა B5G-ის და პერსპექტიულად, 6G ქსელებისთვის. ამ თავში ჩვენ თავდაპირველად წარმოვადგენთ MTD-ის, როგორც თავდაცვის მნიშვნელოვან ელემენტს მომავალი ქსელებისთვის, რასაც მოჰყვება მსჯელობა, თუ როგორ შეიძლება განხორციელდეს ეს ინტეგრაცია. შემდეგ ჩვენ განვიხილავთ სტანდარტიზაციის პერსპექტივას, რათა განვსაზღვროთ მიმდინარე აქტივობები და პოტენციური სამომავლო ძალისხმევა; მოვიყვანთ კონკრეტულ მაგალითს, რომელიც დაფუძნებულია ევროპის სატელეკომუნიკაციო სტანდარტების ინსტიტუტის (ETSI) NFV-SEC სპეციფიკაციებზე. დაბოლოს, წარმოვადგენთ ძირითად კვლევით გამოწვევებს და კვლევის მიმართულებებს MTD-ში ინტეგრირებული მომავალი ქსელებისთვის. საერთო ჯამში განხილული იქნება შემდეგი საკითხები:

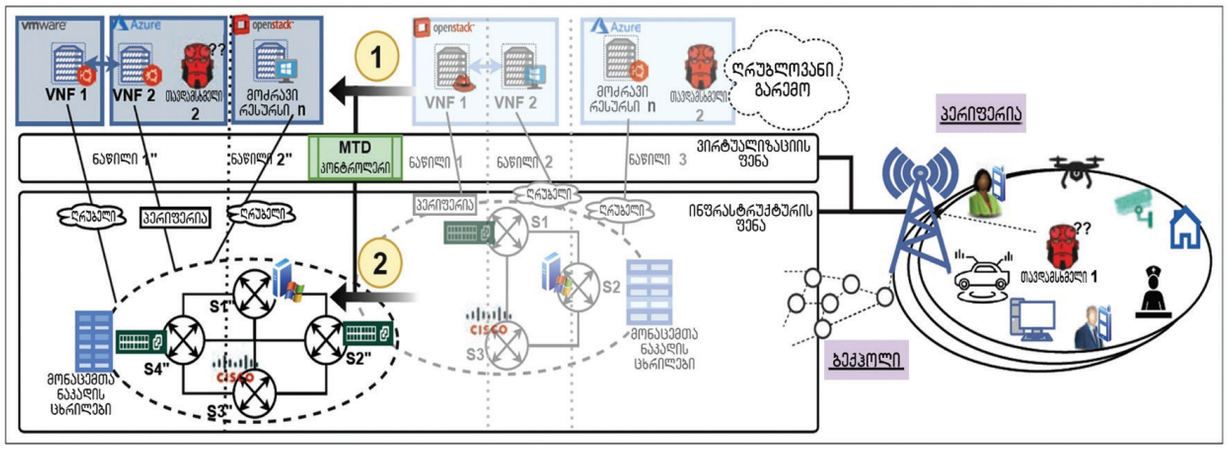
- ჩვენ ვიკვლევთ AI/ML-ზე დაფუძნებულ MTD გადაწყვეტილებებს B5G ქსელებისთვის, გამომდინარე კოგნიტური და ავტომატიზებული უსაფრთხოების პერსპექტივიდან ამ რთული სისტემების მართვისთვის.
- ჩვენ ვაჩვენებთ MTD მოქმედებების მრავალფეროვნებას, რომლებიც შეიძლება შესრულდეს NFV გარემოს სხვადასხვა აბსტრაქციის ფენაზე, რომლებიც ახასიათებს B5G-ის ქსელებს.
- MTD არ განიხილება უსაფრთხოების ზომების მიმდინარე სტანდარტიზაციაში ვირტუალიზებული და SW-ით განსაზღვრული ქსელებისთვის. ჩვენ წარმოვადგენთ სტანდარტიზაციის ასპექტებს, წარმოვადგენთ გაწეულ შესაბამის ძალისხმევას და თუ როგორ შეიძლება MTD-ის ინტეგრირება, ასევე განვიხილავთ MTD-ის პოტენციურ ზემოქმედებას.
- ჩვენ განვსაზღვრავთ და წარმოვადგენთ ძირითად გამოწვევებს და კვლევის მიმართულებებს MTD-ის დანერგვის კუთხით მომავალ 6G ქსელებში.

3.2. ჩატარებული კვლევების მიმოხილვა და ტექნიკური საფუძვლები

MTD პროაქტიულად ცვლის საინფორმაციო და საკომუნიკაციო ტექნოლოგიების (ICT) გარემოს თვისებებსა და კონფიგურაციებს, ავსებს უსაფრთხოების კლასიკურ მიდგომებს, როგორიცაა: firewall, უსაფრთხოების პროტოკოლები, ავთენტიფიკაცია და დაშიფვრა, რაც კიდევ უფრო ზრდის ქსელური

სისტემის დაცვას. MTD მოქმედებები კლასიფიცირდება სამ კატეგორიად: *გადაწყობა*, ქსელის შეცვლა (მაგალითად, მისი ტოპოლოგიის, კონკრეტული ტრაფიკის მოსმენის გასართულებლად) ჰოსტების (მასპინძლების), პროქსი-სერვერების, გადამრთველების, ლინკების და მონაცემთა ნაკადის ცხრილების გადაადგილებით; *მრავალფეროვნება*, ტექნოლოგიური წყობისა და შესრულების გარემოს შეცვლა, როგორიცაა ოპერაციული სისტემები, გადამრთველების სხვადასხვა მომწოდებლით, პროტოკოლებით ან ღრუბლოვანი გარემო, რომელიც ეფუძნება ვირტუალურ კომპონენტებს; და *სიჭარბე*, HW-ის და SW-ის ასლების შექმნა, როგორიცაა დატვირთვის მაბალანსირებელი, მტყუნებების მიმართ მდგრადობის გასაუმჯობესებლად და რისკების შესამცირებლად.

მაგალითად, ნახ. 3.1 წარმოგვიდგენს MTD სტრატეგიების ვიზუალიზაციას და თუ როგორ შეიძლება მათი რეალიზება ვირტუალიზებულ და SW-ით განსაზღვრულ ქსელში. მარკერი 1 აჩვენებს MTD გადაწყობის და მრავალფეროვნების სქემებს, რომლებიც შეიძლება შესრულდეს ღრუბლოვან გარემოში ვირტუალური რესურსების გადასატანად, როგორიცაა ვირტუალური ქსელის ფუნქციები (VNF) და ქსელის ნაწილების კომპონენტების გადატანა ერთი NFV ინფრასტრუქტურიდან (NFVI) მეორეში (მაგალითად, VMware-დან Openstack-ში ან Azure-ში), ან როგორ შეიძლება გადანაწილდეს ქსელის ნაწილების რესურსები სხვადასხვა ღრუბლოვან NFVI-ზე და არ მოხდეს მათი დაჯგუფება ერთ ღრუბლოვან ინფრასტრუქტურაში. მარკერი 2 აღწერს ინფრასტრუქტურის ფენის მუტაციას, რომელიც აკავშირებს ქსელის სხვადასხვა ელემენტს, რაც საშუალებას იძლევა შეიცვალოს ქსელის ტოპოლოგია და პაკეტების ტრაფიკი SW-ით განსაზღვრული ქსელის (SDN) კონტროლერების მონაცემთა ნაკადის ცხრილებით. მრავალფეროვნება შეიძლება დაემატოს გადამრთველის სხვადასხვა მომწოდებლის (მაგალითად, OpenVSwitch, Cisco და Windows გადამრთველების გადაწყობით) ან კომპონენტების გადაადგილებით ქსელის პერიფერიაზე არსებული ლოკალური ღრუბლიდან დისტანციურ ღრუბელში ინტერნეტის საშუალებით.



ნახ. 3.1. MTD სტრატეგიები SW-ით განსაზღვრულ ქსელში

ლიტერატურაში არსებულ კვლევებში შემოთავაზებულია სხვადასხვა მიდგომა გადაწყობის, მრავალფეროვნებისა და სიჭარბის შემოტანის ოპერაციების გამოყენებით, როგორიცაა: ქსელისა და მეხსიერების მისამართების სივრცის რანდომიზაცია, ინსტრუქციების ნაკრების რანდომიზაცია და SW-ის დივერსიფიკაცია. ისინი არსებითად ზრდის სამიზნე სისტემის კონფიგურაციის აღმოსაჩენად საჭირო სირთულეს და დროს, რაც გამოწვეულია საძიებო ზედაპირის გაფართოებით ან თავდასხმის ზედაპირის პროაქტიულად გადაადგილებით. ასევე წარმოდგენილია ინტერნეტის DDoS თავდასხმებისგან მოძრავი სამიზნეების დაცვის მექანიზმი და ახალი MTD სტრუქტურა, რომელიც აუმჯობესებს MTD გადაწყვე-

ტას DDoS თავდასხმების წინააღმდეგ და ახდენს მის ოპტიმიზაციას ღრმა განმტკიცებული სწავლების (DRL) მეშვეობით.

ლიტერატურაში ასევე შესწავლილია MTD სტრუქტურის გამოყენება NFV არქიტექტურაში, რის შედეგადაც ხდება Crossfire DDoS თავდასხმების პრევენცია და ტრაფიკის გადამისამართება ვირტუალურ ჩრდილოვან ქსელებზე მოტყუების მიზნით. ასევე, ღრუბლოვანი ქსელის თავდასხმის გრაფი გამოყენებული იქნა მარკოვის თამაშის მოდელის ზოგადი ჯამის ფორმულირებისთვის და შტაკელბერგის წონასწორობის პრობლემის გადასაჭრელად, რომელიც უზრუნველყოფს ღრუბლოვანი სისტემების დასაცავად უსაფრთხოების რესურსების განთავსების ოპტიმალურ სტრატეგიას. ამ ნამუშევრებისგან განსხვავებით, ქვემოთ შესწავლილია MTD-ის კონცეფციის შემოტანა B5G და 6G ქსელებში კარგად ინტეგრირებული გზით, რათა გააუმჯობესდეს ქსელის ნაწილების და VNF-ების უსაფრთხოება.

განვიხილოთ კიბერუსაფრთხოების კოგნიტური ტექნოლოგიები ქსელებში და ქსელურ სერვისებში. ბოლო დროს ფართო ყურადღება მიიპყრო ML/AI-ის და განსაკუთრებით DL მეთოდების გამოყენებამ, მათი შთამბეჭდავი მახასიათებლებით და მიღწევებით კიბერუსაფრთხოების სფეროში. DRL, როგორც პერსპექტიული ტექნიკა, რომელიც სულ უფრო და უფრო პოპულარული ხდება B5G-ის უსაფრთხოების მიმართულებით, იყენებს ღრმა ნეირონულ ქსელებს (DNN) კლასიკური განმტკიცებული სწავლების (RL) კვლევისა და სწავლების ფაზის დასაჩქარებლად. იგი განსაზღვრავს აგენტებს, რომლებიც იღებენ ჯილდოს/ჯარიმას მოდელირებულ გარემოზე დაყრდნობით, მარკოვის გადაწყვეტილების პროცესის (MDP) გამოყენებით. აქ აგენტი მიზნად ისახავს განსაზღვროს ოპტიმალური პოლიტიკა, რომელიც მას საშუალებას აძლევს მაქსიმალურად გაზარდოს ჯილდო. ამჟამად მიმდინარეობს კვლევები DRL-ის აპლიკაციებზე კიბერუსაფრთხოებისთვის და როგორც უახლესი მაგალითი, წარმოდგენილია სისტემა, რომელიც უზრუნველყოფს კიბერმდგრადობას ავტონომიური მოწინააღმდეგეების და დამცველი აგენტების DRL-თან ინტეგრირებით, მოწინააღმდეგის მიმდინარე და მომავალი მოქმედებების პროგნოზირებისთვის. ეს საშუალებას აძლევს აგენტებს, გამოიყენონ შესაბამისი ავტომატიზებული მეთოდები ასეთი ქმედებების პრევენციისა და შემცირებისთვის.

ანალოგიურად, შემუშავებული იქნა მრავალაგენტიანი RL სტრუქტურა, რათა გადაიჭრას ორ მოთამაშეს შორის საერთო ჯამის თამაშის ამოცანა, რომელიც ფორმულირებულია თავდამსხმელსა და დამცველს შორის. ასევე, შემოთავაზებული იქნა მრავალაგენტიანი RL ალგორითმი, რომელიც იყენებს ბაიესის მიდგომას შტაკელბერგის ძლიერი Q-სწავლების შესაბამისად, რაც აუმჯობესებს MTD-ს ვებაპლიკაციის უსაფრთხოებისთვის. აღნიშნულ შემთხვევაში MTD სისტემის გაურკვევლობის მოდელირებისთვის თავდამსხმელთა ტიპებისა და ნიუანსების შესაბამისად, გამოყენებული იქნა უნიფიცირებული თეორიულ-სათამაშო მოდელი, კერძოდ, ბაიესის ტიპის შტაკელბერგის თამაშები. თუმცა, ეს არ არის ტრივიალური განხორციელება, როგორც აღნიშნულია ქვემოთ მოცემულ გამოწვევებში. ამ კვლევების შესაბამისად, ჩვენ განვიხილავთ უახლეს ML/AI-ის გამოყენებას MTD სტრატეგიების ოპტიმიზაციისთვის ვირტუალიზებულ და SW-ით განსაზღვრულ სატელეკომუნიკაციო ქსელებში და წარმოვადგენთ გამოწვევებს, რომლებსაც ეს ქმნის საიმედო და სტაბილური ავტონომიური უსაფრთხოების მექანიზმის შესაქმნელად.

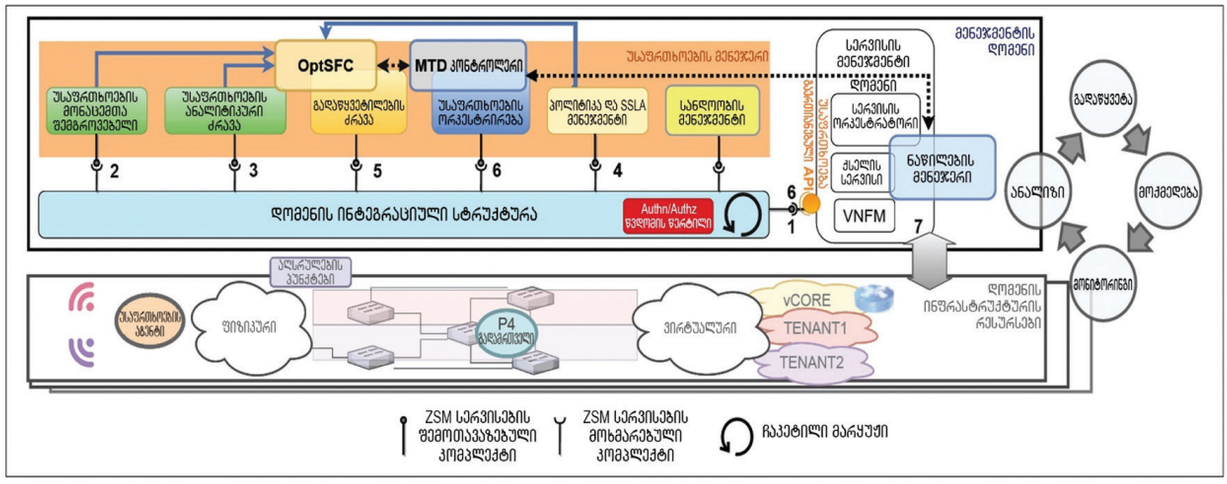
3.3. MTD-ის ინტეგრირება B5G სისტემებში სხვადასხვა დონეზე

როგორც უკვე აღინიშნა, MTD პარადიგმის გამოყენება გამოიწვევს უსაფრთხოების დამატებით ფენას B5G ქსელებში. ამ პარაგრაფში ჩვენ წარმოვადგენთ უსაფრთხოების ჰოლისტიკურ არქიტექტურას B5G სისტემებისთვის და MTD-ის, როგორც უსაფრთხოების პროაქტიული ელემენტის, ინტეგრირებას AI/

ML ჩაკეტილი მარუჯის უსაფრთხოების მიდგომასთან. უსაფრთხოების კონკრეტული მიზნის მისაღწევად, ჩვენ განვიხილავთ ქსელის ნაწილების დაცვას, რომლებიც ემსახურება სხვადასხვა ვერტიკალს და გამოყენების შემთხვევებს. სიტუაცია ბევრად რთული იქნება 6G ქსელებში, ზემოთ განხილული QoS და უსაფრთხოების მოთხოვნების გამო.

მართლაც, რეალურ დროში ჭკვიანი ჩაკეტილ-მარყუჟიანი ორკესტრირების ავტომატიზაციის უზრუნველსაყოფად, შემოთავაზებული მაღალი დონის არქიტექტურა (HLA) დომენის მენეჯმენტის და დომენის ინტეგრაციული სტრუქტურის შემუშავებისთვის იყენებს ETSI-ის ნულოვანი შეხების ქსელის და სერვისის მენეჯმენტის (ZSM) განსაზღვრებას, რათა დააკავშიროს უსაფრთხოების მენეჯმენტის არქიტექტურის სხვადასხვა კომპონენტი და უზრუნველყოს მონიტორინგის, ანალიზის, გადაწყვეტილების მიღებისა და მოქმედების ჩაკეტილ-მარყუჟიანი სამუშაო პროცესი ყველა კომპონენტისთვის.

MTD-ის დინამიკური ხელახალი კონფიგურაციის განხორციელების მიდგომა არის ორი განსხვავებული კომპონენტის გამოყენება: ერთი, ანალიტიკისთვის და კოგნიტური გადაწყვეტილების მიღებისთვის, სახელწოდებით უსაფრთხოების ფუნქციების ოპტიმიზატორი (OptSFC) და მეორე, MTD ქმედებ(ებ)ის შესასრულებლად, სახელწოდებით MTD კონტროლერი. ამ უსაფრთხოების მექანიზმის მოქმედებების ოპერაციული ნაკადი მოიცავს შვიდ მიმდევრობით საფეხურს (მონიშნულია ნახ. 3.2-ზე):



ნახ. 3.2. ჩაკეტილ-მარყუჟიანი და ყოვლისმომცველი უსაფრთხოების არქიტექტურა MTD-ისა და კოგნიტური ფუნქციების გათვალისწინებით

- სერვისის მენეჯმენტის დომენი აგროვებს მონაცემებს მონაცემთა სხვადასხვა წერტილიდან დომენის ინფრასტრუქტურის რესურსების დონეზე (სურათის ქვედა ნაწილი) და გადასცემს მათ უსაფრთხოების მონაცემთა შემგროვებელს.
- უსაფრთხოების მონაცემთა შემგროვებელი აანალიზებს და ამუშავებს „ნედლ“ მონაცემებს და მიაწოდებს მათ უსაფრთხოების ანალიტიკურ ძრავას.
- უსაფრთხოების ანალიტიკური ძრავის სხვადასხვა ანომალიისა და თავდასხმის აღმოჩენის სერვისები წარმოქმნის უფრო მაღალი დონის მონაცემებს, ანუ მეტა-მონაცემებს და აწვდის მათ გადაწყვეტილების ძრავას.
- პოლიტიკისა და „უსაფრთხოების სერვისის დონის შეთანხმების“ (SSLA) მენეჯმენტი განსაზღვრავს MTD-ის ოპერაციების საფუძველს შესაბამისი სერვისებისა და ვერტიკალების მოთხოვნებისა და პოლიტიკის მიწოდებით.
- OptSFC, რომელიც გადაწყვეტილების ძრავის ნაწილია, იყენებს ML/AI ალგორითმებს, როგორი-

ცაა RL და თამაშების თეორია, რათა განისაზღვროს ოპტიმალური სტრატეგია და გადაწყვიტოს შესასრულებელი MTD ქმედებები. მნიშვნელოვანია აღინიშნოს, რომ პროაქტიული სტრატეგიებისთვის OptSFC სულაც არ არის აუცილებელი ამუშავდეს კონკრეტული მოვლენის ან უსაფრთხოების სისტემის გაფრთხილების გამო.

- MTD კონტროლერი, რომელიც არის უსაფრთხოების ორკესტრირების ნაწილი, შემდეგ ახორციელებს გადაწყვეტილებით მიღებულ მოქმედებებს ან ქმედებების კომპლექტს, მათ შორის უსაფრთხოების ორკესტრებისას განსაზღვრული უსაფრთხოების შესაბამისი ფუნქციების ხელახალ კონფიგურაციას და/ან განთავსებას შესაბამის ნაწილებში.
- ნაწილების მენეჯერი აახლებს ქსელის ნაწილის შაბლონს, უკავშირდება რა NFV ორკესტრატორს (NFVO), ინფრასტრუქტურის ვირტუალურ მენეჯერს (VIM), რომელიც პასუხისმგებელია NFVI-ზე და გლობალური ქსელის (WAN) ინფრასტრუქტურის მენეჯერს (WIM).

სანდოობის მენეჯერი პასუხისმგებელია შესრულების გარემოსა და ქსელის ელემენტების სანდოობის გადამოწმებასა და გარანტიაზე, რომლებიც უზრუნველყოფენ რესურსებს ქსელის ნაწილების შექმნისთვის. ამ სქემის მუშაობის რეჟიმი არის ჩაკეტილ-მარყუჟიანი და თვითმართვადი ოპერაციული ნაკადი, რომელიც მოიცავს კოგნიტურ ციკლს {მონიტორინგი, ანალიზი, გადაწყვეტა, მოქმედება} MTD-ის ფუნქციონირებისთვის.

შევისწავლოთ OptSFC და კოგნიტური მეთოდები – AI/ML-ზე დაფუძნებული მართვა. ქვემოთ ჩვენ წარმოვადგენთ OptSFC-ის დიზაინს AI/ML ფუნქციებით, რაც უზრუნველყოფს MTD მუშაობის ადაპტირებულ და ჩაკეტილი მარყუჟით მართვას. OptSFC შეიძლება განხორციელდეს მორგებული მოდელირებული DRL ალგორითმით, რომელიც გამოყენებული იქნება მუდმივად, MTD მოქმედებების ადაპტაციისთვის ქსელის ცვლილებებთან. ამ მიზნით, ოპერაციული გარემო ფორმალურად არის განსაზღვრული თამაშების თეორიის მოდელით MDP-ის გამოყენებით. ამ კონტექსტში, გარემო მოდელირებულია, როგორც რეალურ დროში ფუნქციონირებადი მონიტორინგის სისტემა, რომელიც აანალიზებს ქსელის სტატუსს და მის რესურსებს (მაგალითად, ქსელის ნაწილებს, სერვისებს/აპლიკაციებს და VNF-ებს), რაც დეტალიზებულია მათი აღწერილობით, მნიშვნელობით და სტატუსით: ფუნქციონალური, საეჭვო აქტივობის ან თავდასხმის შემთხვევაში. თავდასხმის დროს, ხელმისაწვდომი მონაცემები თავდასხმის მახასიათებლების შესახებ ემატება ქსელის მდგომარეობას. მნიშვნელოვანია გვახსოვდეს, რომ MTD ასევე მოქმედებს, როგორც პროაქტიული მექანიზმი, რაც იმას ნიშნავს, რომ OptSFC-ს შეუძლია გამოიწვიოს MTD მოქმედებები კონკრეტული თავდასხმის გამოვლენის გარეშე. თუმცა, მოდელი ითვალისწინებს თითოეული რესურსის სტატუსის წონას და MTD მოქმედების აღსრულების ღირებულებას, ვინაიდან სხვადასხვა MTD ქმედებას განსხვავებული ბუნება, ეფექტიანობა და ღირებულება აქვს. OptSFC-ის მთავარი მიზანია შეიმუშაოს სტრატეგია საუკეთესო კომპრომისით QoS ზემოქმედებასა და ქსელის უსაფრთხოებას შორის (და ამ უკანასკნელის სასარგებლოდ მხოლოდ კონკრეტულ შემთხვევაში), თანაც ყოველთვის თავიდან აიცილოს სერვისის შეფერხება.

MDP მოდელის ვარიაციები შეიძლება შემუშავდეს და ფუნქციონირებდეს. საბაზისო მოდელს შეუძლია გამოიყენოს ერთადერთი აგენტი, MTD კონტროლერი, რომელიც მხოლოდ აღიქვამს ქსელის მდგომარეობის ცვლილებას, ფოკუსირებულია პროაქტიულ თავდაცვაზე და თავდასხმის პრევენციაზე. ალტერნატიული მოდელი შეიძლება შეიცავდეს დამატებით აგენტს, კერძოდ თავდამსხმელს, რაც საშუალებას მისცემს MTD კონტროლერს გააუმჯობესოს რეაქტიული დაცვა და შეამსუბუქოს თავდასხმა. გარემო და თამაშების თეორიის მოდელი წარმოადგენს დამატებით პარამეტრებს თავდამსხმელის იდენტიფიკაციისა და მისი სამიზნის პროგნოზირებისთვის. თავდამსხმელთა სტრატეგიები შეიძლება შეი-

ცვალოს დროთა განმავლობაში; ამიტომ, მოდელმა უნდა აღწეროს მაღალი დონის თავდასხმის შაბლონები ძველი და ახალი თავდასხმების იდენტიფიცირებისთვის ქცევების ანალიზით და განზრახვების პროგნოზირებით: დაზვერვა, DoS, ბრძანება და კონტროლი, MitM და ა. შ. ამ მრავალაგენტიანი მოდელის უპირატესობაა ექსპერიმენტების ჩატარების შესაძლებლობა ავტონომიური, მასწავლებლის გარეშე სწავლების სისტემის რეალიზაციაზე, კონცეპტუალურად მსგავსი ნეირონული ფიქტიური თვითთამაშის – „წითელი გუნდი/ლურჯი გუნდი“ სიმულაციით, სადაც ორი აგენტი (MTD კონტროლერი და თავდამსხმელი) ავტონომიურად სწავლობს „ნულიდან“, დომენის წინასწარ განსაზღვრული ცოდნის გარეშე, გარდა თამაშის წესებისა.

3.4. სტანდარტიზაციის აქტივობები და მომავლის პერსპექტივა

სტანდარტიზაციის კუთხით, MTD არ ყოფილა რაიმე დაკავშირებული საქმიანობის ძირითადი საგანი სტანდარტების შემმუშავებელ ორგანიზაციებს შორის. თუმცა, განსახორციელებლად, MTD იყენებს სამ არსებულ ტექნოლოგიას: AI/ML-ს, NFV/SDN-ს და ქსელის ავტომატიზაციას, რომლებზეც მუშაობა სტანდარტიზაციის სხვადასხვა აქტივობის ფარგლებში მიმდინარეობს. ეს სამი მექანიზმი საშუალებას მისცემს MTD-ის, გამოყენებულ იქნეს პრაქტიკაში და მათი სწორი ფუნქციონირება უკვე ქმნის ახალ გამოწვევებსა და მოთხოვნებს 5G და B5G ქსელებში. ამ მექანიზმების შესახებ გამოქვეყნდა ტექნიკური მახასიათებლებისა და ანგარიშების მნიშვნელოვანი რაოდენობა. ამ პარაგრაფში ჩვენი განხილვის სარგებელი ორმხრივია: პირველი დაკავშირებულია სამომავლო ქსელების პერსპექტივასთან: ჩვენ განვსაზღვრავთ სტანდარტიზაციის მცდელობებს, რომლებიც გადამწყვეტი იქნება B5G სისტემებისთვის. მეორე, შედარებით მოკლევადიანია: ჩვენ ასევე ხაზს ვუსვამთ, თუ როგორ შეიძლება მათი გამოყენება/განვითარება MTD-ის ინტეგრირებისთვის განვითარებად 5G ქსელებში. შესაბამისად, ქვემოთ მოცემული კონკრეტული მაგალითი ორივე მიზანს ემსახურება.

5G-ის ძირითადი ქსელის სერვისზე დაფუძნებულ არქიტექტურაში, 3GPP-მ შეიმუშავა AI/ML-ის გამოყენება ქსელის მონაცემთა ანალიზის ფუნქციის (NWDAF) შემოტანით. ამ ფუნქციის მიზანია ქსელის სტატუსისა და მომხმარებლის ქცევის ანალიტიკის შემუშავება და წარმოდგენა, ქსელის ანალიტიკური ინფორმაციის მიწოდება ქსელის სხვა ფუნქციებისთვის.

3GPP SA3-მ ახლახან დაიწყო მუშაობა ტექნიკური ანგარიშის პროექტზე (TR 33.866 – ქსელის ავტომატიზაციის უსაფრთხოების ასპექტების შესწავლა 5G სისტემისთვის, ფაზა 2 (გამოშვება 17)), რომელიც განსაზღვრავს უსაფრთხოების საკითხებს, მოთხოვნებსა და გადაწყვეტილებებს, ფოკუსირებულია ქსელის ნაწილებად დაყოფაზე და იკვლევს, თუ როგორ უნდა იქნეს გამოყენებული შემოთავაზებული NWDAF ზოგიერთი შერჩეული გამოყენების შემთხვევაში. ამ ტიპის ფუნქციონირება შეიძლება გაფართოვდეს და განიხილებოდეს MTD-ის მომდევნო იტერაციებში, რომლებიც მიზნად ისახავს B5G ქსელების დანერგვას.

ETSI-სთან დაკავშირებით, შეიქმნა რამდენიმე ინდუსტრიული სპეციფიკაციის ჯგუფი (ISG), რათა აწარმოონ კვლევები და იმუშაონ 5G ქსელების ძირითად ტექნოლოგიებზე, კერძოდ, NFV (ETSI NFV), AI (ETSI ISG ხელოვნური ინტელექტის უსაფრთხოების უზრუნველყოფა (SAI), ETSI ISG ექსპერიმენტული ქსელური ინტელექტი, ENI), ასევე ქსელებისა და სერვისების ავტომატიზაცია (ETSI ZSM ISG). ამასთან დაკავშირებით, NFV-SEC WG იძლევა სისტემატურ რეკომენდაციებს NFV ტექნოლოგიის უსაფრთხოებასთან დაკავშირებულ საკითხებზე და ავითარებს ინდუსტრიის შესაბამის სპეციფიკაციებს. 2014 წლიდან NFV-SEC WG-მ გამოაქვეყნა რამდენიმე ჯგუფის სპეციფიკაციები (GS) და ანგარიშები (GR). კონკრეტულად, ETSI NFV-ის მე-3 და მე-4 გამოშვებებზე მუშაობის პროცესი უფრო მეტად იყო ფოკუსირებული

უსაფრთხოების სპეციფიკაციებზე, ვინაიდან NFV პლატფორმები ახლა უფრო მომწიფებულია მახასიათებლების, შესაძლებლობებისა და მოცულობის თვალსაზრისით. ეს სპეციფიკაციები მნიშვნელოვანია, როგორც ფოკუსირების წერტილები MTD შესაძლებლობების გაფართოებისა და გააქტიურებისთვის, როგორც 5G, ასევე B5G სისტემებისთვის.

ETSI ZSM ISG დაარსდა 2017 წელს, რათა განესაზღვრა სერვისის მიწოდების გამჭოლი ქსელური ავტომატიზაციისა და სიცოცხლის ციკლის მართვის სპეციფიკაციები უაღრესად ჰეტეროგენულ ქსელურ გარემოში, როგორიცაა 5G და მომავალი 6G სისტემები. ETSI ZSM განსაზღვრავს ZSM სტრუქტურას, რომელიც საშუალებას აძლევს ქსელს თვითოპტიმიზაცია მოახდინოს მითითებული SLA-ების მიხედვით. ქსელი იყოფა ცალკეულ მმართველ დომენებად, რომელთაგან თითოეულს აქვს საკუთარი მუშაობის პროცესი ჩაკეტილი მარყუჟით, რომელიც ექვემდებარება სერვისის მართვის ყოვლისმომცველ დომენს და რომელიც, თავის მხრივ, მომხმარებლისთვის სერვისების სრულ მიწოდებაზეა პასუხისმგებელი. ETSI ZSM ეფუძნება AI-ის და ქსელის ნაწილებად დაყოფას, რათა მოახდინოს მისი ხედვის რეალიზაცია. უსაფრთხოების კუთხით, ISG ZSM-მა ცოტა ხნის წინ გამოაქვეყნა ETSI GR ZSM 010 სპეციფიკაცია „ZSM სტრუქტურის ზოგადი უსაფრთხოების ასპექტები“, რომელიც შეიცავს მისი მუშაობიდან გამომდინარე საფრთხეების ყოვლისმომცველ ჩამონათვალს.

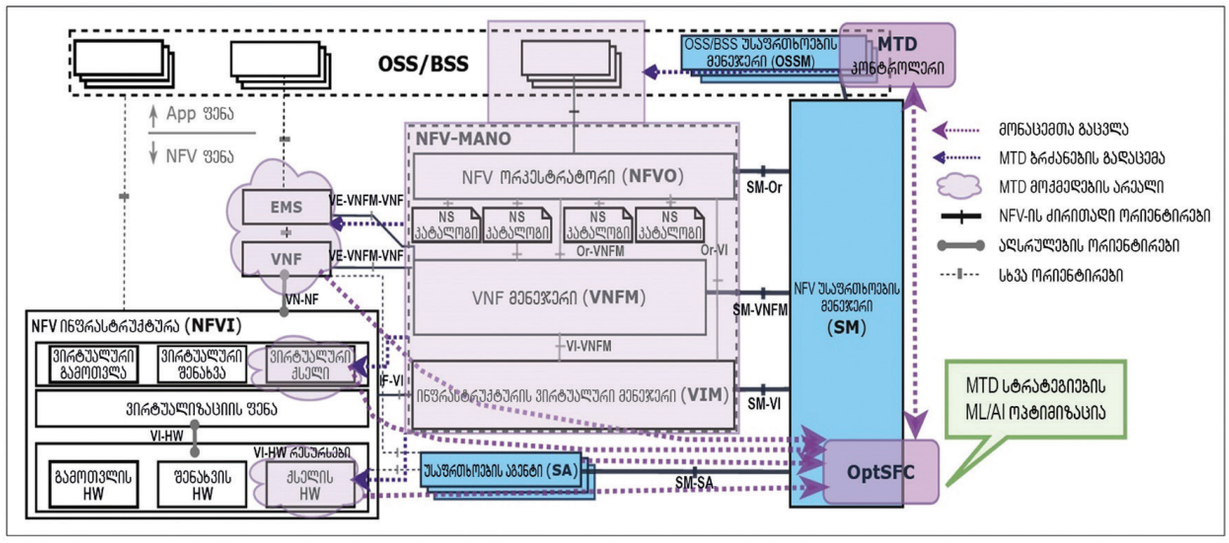
ETSI ISG ENI, რომელიც ასევე 2017 წელს დაარსდა, განსაზღვრავს ქსელის მენეჯმენტის კოგნიტურ არქიტექტურას, რომელიც დაფუძნებულია AI ტექნოლოგიებზე, რათა მოარგოს შემოთავაზებული სერვისები მომხმარებლის დინამიკურ საჭიროებებს, სისტემის პირობებსა და კონტექსტზე დამოკიდებულ ბიზნესმიზნებს. ამ ISG-მ შეიმუშავა გამოყენების მრავალი შემთხვევა, მათ შორის ქსელის უსაფრთხოება, სადაც ქსელური თავდასხმის გამოვლენა და კონტრზომები იმართება ENI სისტემის მიერ ინტელექტუალური და ადაპტიური გზით. სხვა დაკავშირებული ჯგუფი, ETSI ISG SAI, ჩამოყალიბდა 2019 წელს და მიზნად ისახავს შეიმუშაოს ტექნიკური სპეციფიკაციები საფრთხეების შესამცირებლად AI-ის ფართო გამოყენების გამო, ისევე როგორც შეამციროს სხვა AI სისტემების მიერ გამოწვეული საფრთხეები მოცემული AI სისტემებისთვის. შესაბამისად, მან აიღო ამოცანები AI-ის საფრთხის განსაზღვრის, გამოყენების შესაბამისი შემთხვევებისა და შესაბამისი შემამსუბუქებელი ღონისძიებების იდენტიფიცირებისა და მონაცემთა ეფექტიანი და უსაფრთხო გაზიარებისთვის შესაძლო რეკომენდაციების შემუშავების შესახებ. როგორც გაეროს ICT სააგენტომ, ტელეკომუნიკაციის საერთაშორისო კავშირმა (ITU) ჩამოაყალიბა სტანდარტიზაციის ITU-T ფოკუს-ჯგუფი – ML, მომავალი ქსელებისთვის (FG-ML5G), რომელიც მუშაობს ML-ის ტექნიკურ მახასიათებლებზე მომავალ ქსელებში, რაც მოიცავს ინტერფეისებს სისტემის ელემენტებს შორის, ქსელის არქიტექტურებს, პროტოკოლებს, ალგორითმებსა და მონაცემთა ფორმატებს.

მნიშვნელოვანია აღინიშნოს, რომ ინდუსტრიის ბევრმა ფორუმმა, მათ შორის NGMN, 5G Americas, 5G-PPP და GSMA და სააგენტოებმა, როგორიცაა ENISA და FCC, გამოაქვეყნეს ტექნიკური ანგარიშები 5G ქსელებში გამოვლენილი პოტენციური საფრთხეების შესახებ. ეს საფრთხეები მიეკუთვნება 5G ტექნოლოგიების მთელ სპექტრს, მათ შორის NFV, AI და ქსელის დანაწევრებას და გავლენას ახდენს B5G სისტემებზე. ეს ანგარიშები იძლევა საფრთხეების ყოვლისმომცველ სურათს, სადაც MTD, როგორც ახალი ტექნოლოგია, შეიძლება განთავსდეს თავდასხმის სხვადასხვა სცენარის შესამსუბუქებლად.

3.4.1. ინტეგრირება NFV უსაფრთხოების არქიტექტურაში

ETSI NFV სტანდარტები განსაზღვრავს შესაბამის არქიტექტურას MTD-ის ინტეგრირებისთვის 5G და B5G ქსელებში. აღნიშნული ISG ამჟამად მუშაობს NFV არქიტექტურის უსაფრთხოების გაუმჯობესე-

ბაზე, დამატებითი კომპონენტებით, როგორიცაა ოპერაციული/ბიზნესის მხარდაჭერის სისტემის (OSS/BSS) მენეჯერები (OSSM), NFV უსაფრთხოების მენეჯერები (SM) და უსაფრთხოების აგენტები (SA). ეს ელემენტები განსაზღვრულია ETSI GS NFV-SEC 024-ით, რომელიც ჯერ კიდევ დამუშავების პროცესშია და აქამდე არ გახდა ჰარმონიზებული სტანდარტი. MTD შეიძლება ეფექტიანად იყოს ინტეგრირებული ამ არქიტექტურაში, როგორც ნაჩვენებია ნახ. 3.3-ზე. NFV-SEC 024 პროექტით განსაზღვრული დამატებითი ელემენტები ნაჩვენებია ლურჯი ფერით.



ნახ. 3.3. MTD უსაფრთხოების ინტეგრირება ETSI NFV უსაფრთხოების არქიტექტურაში (ETSI NFV, გამოშვება 4, უსაფრთხოება; უსაფრთხოების მართვის სპეციფიკაცია: GS NFV-SEC 024 v.0.0.5) (აკრონიმები მოცემულია წიგნის ბოლოს, განყოფილებაში: აბრევიატურები და აკრონიმები)

NFVI დონეზე ამ ინტეგრირებით, MTD კონტროლერი შეცვლის ვირტუალურ ქსელს ღრუბლოვან გარემოში ან მონაცემთა ნაკადს ქსელის აპარატურულ აღჭურვილობაზე VIM-ისა და მისი SDN კონტროლერის გამოყენებით. ამის ნაცვლად, VNF ფენაზე მას შეუძლია გადაიტანოს ცალკეული VNF ან მთელი ქსელის სერვისები ერთი NFV ინფრასტრუქტურიდან მეორეზე. ეს MTD „სათამაშო მოედნები“ წარმოდგენილია ნახ. 3.3-ზე ღია მელნისფრად. ქსელის სერვისის პროვაიდერს შეუძლია გაასუმჯობესოს MTD-ის ეფექტები VIM-ების გამოყენებით, რომლებიც მართავენ NFVI-ების კომპლექტს, გადაწყობისა და განცალკევების სქემების კომბინაციით ღრუბლის დონეზე (როგორც ადრე იყო ნაჩვენები ნახ. 3.1-ზე). კიდევ ერთი შესაძლებლობაა WIM-თან კომუნიკაცია, რათა დინამიკურად შეცვალოს სატრანსპორტო ქსელის გრაფი, რათა WIM-მ შეძლოს 5G WAN რესურსების დაჯავშნა და უზრუნველყოს დინამიკური, გამჭვირვალე E2E კავშირი SDN წესების გამოყენებით.

3.4.2. MTD-ის ღირებულებასა და ეფექტიანობას შორის კომპრომისი

MTD მოქმედებები, როგორიცაა VM მიგრაცია და VM გადატვირთვა შეიძლება ოპტიმიზებული იყოს, მათი QoS და ქსელის მუშაობის ოვერჰედების შესამცირებლად; მაგალითად, შესაძლებელია VNF-ის სარეზერვო ეგზემპლარის გამოყენება საწყისი ეგზემპლარის გადაადგილებისას. VNF-ები ასევე შეიძლება განთავსდეს კონტეინერებში და არა VM-ებში, შეასრულონ კონტეინერების მართვა და ორკესტრირება VNF-ის უფრო სწრაფი განთავსებისთვის და უფრო სწრაფი რეაგირებისთვის მეორე დღის ოპერაციებზე (ოპერაციები შესრულებული VNF-ზე, მისი ფუნქციონირების დროს). კონტეინერირებული VNF-ები

დეტალურად იქნა განხილული და განსაზღვრული ETSI NFV-ის მიერ GR NFV IFA 029-ში და GR NFV IFA 040-ში.

OptSFC კოგნიტურ სისტემას ასევე შეუძლია განიხილოს MTD მოქმედებების შესრულება, რომელიც დაფუძნებულია ფუნქციურ ფაქტორებზე, როგორიცაა: QoS, ქსელის ნაწილებისა და VNF-ების გადაადგილებით, პერიფერიული გამოთვლითი შესაძლებლობების მეშვეობით. მრავალჯერადი წვდომის პერიფერიული გამოთვლები კონტენტსა და აპლიკაციებს საშუალებას აძლევს განლაგდეს ოპერატორის RAN-თან უფრო ახლოს, კომპიუტერულ გარემოში, რაც ამცირებს მონაცემთა ტრაფიკსა და შეყოვნებას. MEC დაფუძნებულია ETSI NFV არქიტექტურაზე, რომელიც სტანდარტიზებულია ETSI GS MEC 003-ში, რაც მას შესაფერის ტექნოლოგიად აქცევს MTD-ის განსათავსებლად და B5G და 6G ქსელების უსაფრთხოების უზრუნველსაყოფად.

ვინაიდან ეს მუტაციები ხორციელდება სხვადასხვა აბსტრაქციულ ფენაზე, MTD მოქმედებებს აქვს სხვადასხვა ფასი. ეს, MTD ქმედებების შემცირებულ შესაძლებლობებთან ერთად (მახასიათებლებთან დაკავშირებული პრობლემების გამო), გასათვალისწინებელია OptSFC კომპონენტის ოპტიმიზაციის სტრატეგიის შემუშავებისას და გადაწყვეტილების მიღებისას MTD კონტროლერის ღირებულების/ეფექტურობის თანაფარდობის გასაუმჯობესებლად, უსაფრთხოებასა და მახასიათებლებს შორის კარგი კომპრომისის პოვნის მიზნით. ეს არის მნიშვნელოვანი კვლევითი გამოწვევა, როგორც ქვემოთ იქნება ნაჩვენები.

3.5. გამოწვევები და მომავალი კვლევის მიმართულებები

ეს პარაგრაფი ყურადღებას ამახვილებს კვლევის გამოწვევებზე, რომლებიც განხილულ უნდა იქნეს MTD-ის ინტეგრირებისას, როგორც უსაფრთხოების არქიტექტურის ნაწილი B5G და 6G ქსელებისთვის. ისინი განხილულია ქვემოთ და ასევე შეჯამებულია ცხრილში 3.1.

3.5.1. არქიტექტურული გამოწვევები

ლიტერატურაში შესწავლილი MTD მეთოდები ჩვეულებრივ ფოკუსირებულია MTD-ის ცალკეულ ასპექტზე და მასთან დაკავშირებულ უსაფრთხოების მოთხოვნებზე. სრული სტეკის და სრული სივრცით-დროითი მოქმედების სივრცის ინტეგრაცია და გამოყენება (მაგალითად, ცოცხალი VM მიგრაცია, ოპერაციული სისტემის დივერსიფიკაცია, ჰიბრიდული მრავალფეროვნება, გადაწყობა და სიჭარბის შემოტანა) ვირტუალიზებულ ინფრასტრუქტურაში (SW-ის სტეკის მრავალი ფენა) თანდაყოლილი ენტროპიის მაქსიმიზაციის მიზნის მისაღწევად MTD-სთვის ჯერ კიდევ ნაკლებად არის გასაგები.

სწავლებაზე დაფუძნებული უსაფრთხოების ავტონომიური და აქტიური ოპტიმიზაცია რთული არქიტექტურული გამოწვევაა სერვისების, ინფრასტრუქტურისა და ოპერატიული მოთხოვნების არაერთგვაროვნების გამო. ერთ-ერთი მთავარი კითხვაა, თუ როგორ გავაერთიანოთ MTD და AI/ML სხვადასხვა ფენის დასაცავად 6G-ში, როდესაც ჩვენ ვქმნით შემდეგი თაობის უსადენო ქსელებს. როგორც ზემოთ აღინიშნა, კიდევ ერთი მთავარი გამოწვევა არის ის, თუ როგორ განვითარდება მიმდინარე 5G სპეციფიკაციები, რათა შესაძლებელი გახდეს 6G-ის დანერგვა. ეს ბოლო საკვლევი კითხვა მოიცავს საჭირო ახალი ინტერფეისებისა და ახალი შესაძლებლობების იდენტიფიცირებას, დიზაინს ქსელის ფუნდამენტურ ელემენტებში და უსაფრთხოების მართვის სტრუქტურაში, რომელიც გაჩნდება 6G-ით.

3.5.2. გამოწვევები 6G აპლიკაციებისა და მოთხოვნების გამო

გათვალისწინებული 6G აპლიკაციები და შესაბამისად, მოთხოვნები შექმნის QoS-ის და სერვისის დონის დიდ გამოწვევებს. ამასთან დაკავშირებით, კიდევ უფრო გაუმჯობესებული მობილური ფართოზოლოვანი (FeMBB) ქსელიდან მოელიან, რომ მონაცემთა უკიდურესად მაღალი სიჩქარე 6G ვერტიკალებს მოემსახურება. თუმცა, ასეთი ტერაბიტი წამში გადაცემის სიჩქარე წარმოუდგენელი ტესტია ტრაფიკის დამუშავებისთვის ქსელის უსაფრთხოების ფუნქციებში. ეს აუცილებლობა ასევე ეწინააღმდეგება MTD გადაწყვეტილებებს, რადგან მათ ექნებათ დამატებითი ოვერჰედები მონიტორინგის, მოვლენების დამუშავებისა და კონტრზომების აღსრულების თვალსაზრისით. ამიტომ, განაწილებული MTD გადაწყვეტილებების შემუშავება და დანერგვა მნიშვნელოვანი კვლევის თემაა, რადგან ტრაფიკი უნდა დამუშავდეს ადგილობრივად და ძალზე სწრაფად გადაიცეს ქსელის სხვადასხვა წერტილში.

კვლევითი გამოწვევები	კვლევის ძირითადი თემები	საკვანძო პუნქტები
არქიტექტურული გამოწვევები	სრული სტეკის და სრული სივრცით–დროითი მოქმედების სივრცე MTD-სთვის	ვირტუალიზაცის სხვადასხვა ფენების ექსპლუატაცია MTD ენტროპიის მაქსიმალურად გაზრდის მიზნით
	დაბალი სირთულის ინტეგრაცია	ეფექტიანი MTD მექანიზმები და ინტერფეისის დიზაინი ქსელის მასშტაბურობისა და მოქნილობისთვის
	5G სპეციფიკაციების ევოლუცია 6G-მდე	ახალი არქიტექტურული ელემენტები და შესაძლებლობები, რომლებიც საჭიროა AI/ML-ის, ორკესტრირებისა და ვირტუალიზაციის არსებულ სპეციფიკაციებში
6G აპლიკაციები და მოთხოვნები	FeMBB	ოვერჰედის მინიმიზაცია; როგორ განვახორციელოთ განაწილებული MTD გადაწყვეტილებები ადგილობრივი უსაფრთხოებისთვის
	ექსტრემალური მასობრივი კავშირი	მასშტაბურობა, გავლენა OSS/BSS-ზე მონიტორინგისა და აღრიცხვისთვის
	ERLLC/eURLLC	შეყოვნების მინიმიზაცია შეფერხებისადმი მგრძნობიარე აპლიკაციებისთვის
AI/ML-თან დაკავშირებული გამოწვევები	უკონტროლო თვითმართვადი RL	რეპრეზენტაციული მარკოვის მოდელი, AI-ის ახსნადობა და უკონტროლო სწავლების შეფასება
	ეფექტიანი მოდელები და ოპტიმალური სამოქმედო მენეჯმენტი	რა/სად/როდის/როგორ იმოძრაოს, პროაქტიული და რეაქტიული სქემების კომბინაცია და მოქმედების მინიმალისტური იძულება
	უსაფრთხო AI კიბერუსაფრთხოებისთვის	AI-ის ეთიკა და პასუხისმგებლობა, AI-ის უსამართლობა, კონფიდენციალურობა, სანდო მონაცემთა მხარდაჭერა და ფრთხილი RL მოდელირება
ორკესტრირება და მენეჯმენტი	ჰეტეროგენული ქსელის არქიტექტურები	სხვადასხვა MTD ელემენტების სინქრონიზაცია/გაერთიანება მრავალი მომხმარებლის გარშემო
	ფუნდამენტური საზღვრები	უსაფრთხოების მენეჯმენტის იდენტიფიკაცია MTD-ით მიღწევადი შესაძლებლობებით
	საიმედოობა	თანმიმდევრული მწარმოებლურობა და რობასტულობა უსაფრთხოების სხვადასხვა ინციდენტის პირობებში

ცხრილი 3.1. კვლევის გამოწვევები და მიმართულებები MTD-სთვის 6G უსაფრთხოების მენეჯმენტში

ყველაფრის ინტერნეტის (IoE) გაჩენით, umMTC მოიცავს ექსტრემალური მასობრივი კავშირის გამოყენების შემთხვევებს, მათ შორის კრიტიკულ შემთხვევებს, რომლებსაც აქვთ ბევრად უფრო მკაცრი უსაფრთხოების მოთხოვნები ამჟამინდელ 5G ანალოგებთან შედარებით. ამასთან დაკავშირებით, საოცრად მრავალფეროვანი შესაძლებლობების მქონე მოწყობილობები და პროგრამული ელემენტები საფრთხეს უქმნის უსაფრთხოების გადაწყვეტილებების გამოყენებას. მიუხედავად იმისა, რომ ტექნოლოგიური შესაძლებლობები კიდევ უფრო განვითარდება, კვლავ იქნება რესურსებით შეზღუდული მოწყობილობები, განსაკუთრებით უკიდურესად მომთხოვნი აპლიკაციების გაჩენის გამო. როგორც მობილურ ქსელს, 6G-ის ასევე, საქმე ექნება ბევრად უფრო მაღალ მობილურობასთან, რაც საფრთხეს უქმნის უსაფრთხოების ზომების გავლენას დაცვაზე, პერიფერიაზე არსებული ცვლილებების გამო. umMTC-ის მსგავსად, ERLLC/eURLLC-ის მაღალი საიმედოობა და დაბალი შეყოვნების მოთხოვნები აქცევს MTD სამუშაო ნაკადების გავლენას შეყოვნებაზე მნიშვნელოვან საკვლევ თემატიკად. მაღალი საიმედოობა ასევე მოითხოვს მაღალეფექტიან უსაფრთხოების გადაწყვეტილებებს, რომლებიც იცავს სერვისების ხელმისაწვდომობას ექსტრემალურად მაღალ დონეზე. ეს მოთხოვნა ასევე გავლენას ახდენს MTD გადაწყვეტილებების დიზაინზე, როგორიცაა DDoS-ით ორიენტირებული დაცვის მიზნები.

3.5.3. AI/ML-თან დაკავშირებული გამოწვევები

დღეისათვის არ არსებობს გეგმა სწავლებაზე დაფუძნებული ოპტიმიზებული MTD-ის დიზაინისა და მუშაობისთვის ფართომასშტაბიანი ქსელის სცენარებისთვის. მიუხედავად იმისა, რომ RL-ზე დაფუძნებული MTD გვპირდება თვითრეგულირებად ავტონომიურ ოპერაციას და კიბერსაფრთხეების შემსუბუქებას, მისი ფუნდამენტური უპირატესობები და გავლენა არ არის გამოვლენილი უსაფრთხოების სხვადასხვა სცენარში. RL-თან ურთიერთობისას, კომპლექსური მოდელები, რომლებიც იყენებენ მრავალაგენტურ DRL-ს, კიდევ უფრო ზრდის სისტემის მოთხოვნებს, რადგან უფრო მაღალი ხარისხის მონაცემებია საჭირო უსაფრთხოების აგენტებიდან და მონიტორინგის სისტემებიდან სწავლების ალგორითმებისთვის. უკონტროლო RL თვითმართვადი სიმულაციებით, მოითხოვს ფრთხილად მოდელირებას, რათა თავიდან იქნეს აცილებული არარეალური გამოცდილება, საიდანაც აგენტები სწავლობენ შეუსაბამო სტრატეგიებს, რომლებიც არ გამოიყენება რეალურ სისტემაში. ამ პრობლემისთვის საჭიროა AI-ის ახსნა-განმარტების დამატებითი ცნება, რათა უკეთ შეფასდეს უკონტროლო მოდელები.

კიდევ ერთი მთავარი გამოწვევაა MTD ეფექტიანობის გაუმჯობესება, რაც მიიღწევა MTD ოვერჰედის მინიმუმამდე შემცირებით, მხოლოდ აუცილებელი და სასარგებლო მუტაციების შესრულებით, ქსელის მდგომარეობისა და რეალურ დროში რისკების, საფრთხეების ანალიზის საფუძველზე. ასეთი ეფექტიანობის გაზომვა ასევე გამოწვევაა, რადგან ის განისაზღვრება MTD მოქმედების კონკრეტული ღირებულებით და მისი ეფექტიანობით კონკრეტული თავდასხმის წინააღმდეგ, განსაკუთრებით MTD მოქმედებებისა და თავდასხმების ყველა კომბინაციისთვის. პროაქტიული (ანუ თავდასხმის ზედაპირის შეცვლა თავდასხმამდე) და რეაქტიული (ანუ თავდასხმის დროს თავდასხმის ზედაპირის შეცვლა და ზემოქმედების მინიმუმამდე დაყვანა) მოქმედებების თანაცხოვრება, რომელსაც მხარს უჭერს ქსელის ონლაინმონიტორინგი სიტუაციური ცნობიერებისთვის, ჯერ კიდევ უნდა იყოს გამოკვლეული 6G ქსელებისთვის. AI/ML-თან დაკავშირებულ ბევრ სხვა კლასიკურ პრობლემას აგვარებენ სტანდარტების შემამუშავებელი და სხვა სამუშაო ჯგუფები. ამის მაგალითია AI-ის ეთიკის ჯგუფი, რომელიც პასუხისმგებელია AI-ის წარუმატებლობის შემთხვევებზე, როგორიცაა: AI-ით გამოწვეული უსამართლობის თავიდან აცილება (მაგალითად, ზოგიერთი მომხმარებლის ან აპლიკაციის „შიმშილის“ თავიდან აცილება), მგრძნობიარე მონაცემების გაჟონვის პრევენცია (მაგალითად, როდესაც ML ფუნქციები ნაწილ-

დება ქსელში) და წინააღმდეგობა მონაცემთა „შხამიანი“ ინექციების მიმართ (მაგალითად, არასაჭირო MTD მოქმედებების შემცირება, რომლებიც ანელებს სისტემას და იწვევს DoS თავდასხმას).

3.5.4. ორკესტრირება და მენეჯმენტის გამოწვევები

MTD-ის კორელაცია ქსელის ნაწილებად დაყოფასთან, B5G-სა და 6G-ში წარმოადგენს გამოწვევას მენეჯმენტისა და ორკესტრირების სისტემებისთვის. ფაქტორები, რომლებიც გავლენას ახდენენ სტრუქტურების უნარზე, გაუმკლავდნენ დაწესებულ მოთხოვნებს, ძირითადად, არის სიჩქარე, იზოლაცია, ქსელის ნაწილის ტოპოლოგიის სირთულე, სანდოობა და ლოკალიზაცია. პირველი ფაქტორი დაკავშირებულია საორკესტრო სტრუქტურის შესაძლებლობასთან, პროაქტიულად ან რეაქტიულად შეცვალოს ნაწილის ტოპოლოგია, რომელიც ინარჩუნებს სერვისის გრაფიკს სერვისის მუშაობის დროს. მეორე ფაქტორი არის იზოლაცია, ანუ იზოლაციისა და სანდოობის შენარჩუნება ნაწილის ტოპოლოგიის ცვლილებების პროცესში. ქსელის ნაწილის ტოპოლოგიის სირთულე ზრდის სასიგნალო ოვერჰედს, რაც გავლენას ახდენს ტოპოლოგიის ინსტანციებს შორის დროულ გადასვლაზე. MTD მოქმედებს მომზადებული და შექმნილი ქსელის ნაწილზე და ცვლის უზრუნველყოფილი რესურსების მდებარეობებს, ცვლის ქსელში გზას და შესრულების გარემოს; ასეთი სანდოობის მენეჯმენტი ქმნის გამოწვევას, რამაც შეიძლება გავლენა მოახდინოს ერთი კონფიგურაციიდან მეორეზე გადასასვლელად საჭირო დროზე, განსაკუთრებით მრავალდომენურ სცენარებში სხვადასხვა ოპერატორის ქსელით. დაბოლოს, მიგრაციისა და მუტაციების ლოკალიზაცია, რომელიც უნდა მოხდეს ყოველი გადასვლისთვის, ასევე ქმნის გამოწვევებს. მაგალითად, ღრუბლოვანი ინფრასტრუქტურის შიგნით ქსელის ნაწილის ტოპოლოგიის მუტაცია (მაგალითად, მიგრაცია ერთი კვანძიდან მეორეში) ნაკლებად მოთხოვნადია, ვიდრე სხვა ღრუბლოვან ინფრასტრუქტურაში მიგრაცია.

3.6. მესამე თავის დასკვნა

MTD დაფუძნებულია უსაფრთხოების ინსტრუმენტებზე, რომლებიც შექმნილია სპეციალურად მობილური მოწყობილობების კიბერსაფრთხეების აღმოსაჩენად და მათგან თავის ასარიდებლად. ისინი აანალიზებენ აპლიკაციების მახასიათებლებს და რეაგირებენ საფრთხეებზე რეალურ დროში, რაც უზრუნველყოფს ქსელში ჩართული ყველა მოწყობილობის რისკის დონის ხილვას. ამ თავში ჩვენ წარმოვადგინეთ და განვიხილეთ MTD, როგორც მთავარი პროაქტიული თავდაცვის ელემენტი ეფექტიანი და ყოვლისმომცველი უსაფრთხოების განსახორციელებლად B5G ინფრასტრუქტურისა და სერვისების დასაცავად. ჩვენ ასევე წარმოვადგინეთ კვლევის შესაბამისი გამოწვევები და სამომავლო კვლევის მიმართულებები სტანდარტიზაციის პერსპექტივის ჩათვლით.

თავი 4. ადაპტიური და დინამიკური უსაფრთხოება ხელოვნური ინტელექტის შემცველ ენერგოეფექტიან 6G ქსელებში

4.1. შესავალი

5G ფიჭური ქსელის გლობალურ კომერციალიზაციასთან ერთად, საყოველთაო ინტერესი 6G ფიჭური ქსელის მიმართ ჩნდება AI-ის განვითარებიდან და ფართო გამოყენებიდან გამომდინარე. მონაცემთა სიჩქარის, შეყოვნების, საიმედოობისა და ქსელის დაფარვის მუდმივი გაუმჯობესების გარდა, 6G წარმოადგენს რევოლუციურ წინსვლას ყოვლისმომცველი ინტელექტის განხორციელებით, რომელიც 6G არქიტექტურის განუყოფელი ნაწილია. ქსელის ავტონომიური მენეჯმენტიდან დაწყებული, სხვადასხვა ინტელექტუალურ სერვისებამდე, AI-ის შეუძლია აქტიური მონაწილეობა მიიღოს 6G ეპოქის სხვადასხვა ასპექტში, როგორიცაა ყოველდღიური ცხოვრება, ინდუსტრიული წარმოება და ურბანული მენეჯმენტი. მილიარდობით ინტელექტუალური მოწყობილობა ფართოდ არის განლაგებული ხმელეთზე, ჰაერში, ზღვასა და სივრცეში გარემოსთან ურთიერთობისთვის და გადაწყვეტილების მისაღებად ნებისმიერ ადგილას და ნებისმიერ დროს. სერვისები, როგორიცაა: ავტონომიური მართვა, ინტელექტუალური რობოტიკა და ინტელექტუალური სასოფლო-სამეურნეო/ინდუსტრიული წარმოება, შეიძლება გაუმჯობესდეს ხელოვნური ინტელექტის მქონე 6G ქსელებით, ადამიანის ზედმეტი ჩარევის გარეშე, რათა შეამციროს ხელით შრომა და უფრო სწრაფად უპასუხოს სხვადასხვა მოთხოვნას.

თუმცა, პერსპექტიული 6G ქსელი აჩენს უამრავ უსაფრთხოების საკითხს ინტელექტუალური სერვისების მზარდი ავტონომიისა და მათი ღრმა ინტეგრირების გამო ჩვენს ყოველდღიურ ცხოვრებაში. ტრადიციული დაუცველობის გარდა, AI-ის ტრენინგის პროცესზე თავდასხმები ახალ გამოწვევებს ქმნის 6G ქსელისთვის. მაგალითად, თავდამსხმელებს შეუძლიათ შეიყვანონ გაყალბებული მონაცემები მოდელის სასწავლო აუზში, რათა მიღებული გადაწყვეტილების საზღვრები გამოუსადეგარი გახადონ. მოწამლულ მოდელს შეუძლია დააინფიციროს კლიენტის სხვა მოდელები ფედერირებული სწავლების პროცესში, ტრენინგის უკონტროლო პარამეტრების ატვირთვით, ინტეგრაციით და განახლებით არასანდო მომხმარებლებს შორის. ამ მიზნით, გარანტირებული უნდა იყოს ადეკვატური უსაფრთხოება მილიარდობით დაკავშირებული მოწყობილობისა და მილიონობით საბაზო სადგურისთვის. მიუხედავად იმისა, რომ 5G უსაფრთხოების სქემები უკვე განიხილავს სხვადასხვა ტიპის თავდასხმის შესაძლებლობას, აღნიშნული ქსელები ხშირად აკონფიგურირებენ უსაფრთხოების სქემებს უნივერსალური პარამეტრებით (როგორიცაა კრიპტოგრაფიული ალგორითმები და მათი გასაღებების სიგრძეები) ყველა სცენარში.

ამ უნივერსალური სტრატეგიის გამოყენება მარტივია, მაგრამ ის აღარ არის შესაფერისი 6G უსაფრთხოებისთვის ორი მიზეზის გამო: პირველი, მომხმარებლის მოწყობილობებს 6G ქსელში აქვთ უფრო მრავალფეროვანი ტექნიკური შესაძლებლობები და ისინი განლაგებულია უფრო რთულ გარემოში, რომელიც არ არის დაფარული 5G-ით, რაც მოითხოვს უსაფრთხოების შესაბამის ადაპტაციას. მაგალითად, წყალქვეშა მოწყობილობებს, როგორც წესი, აქვთ უფრო შეზღუდული ელექტრომომარაგება, ვიდრე მოწყობილობებს ხმელეთზე, ამიტომ უსაფრთხოების „მსუბუქი“ სქემები სასურველია უფრო ხანგრძლივი მუშაობისთვის; მეორეც, 5G უსაფრთხოებას არ ძალუძს დროში ცვალებადი ატრიბუტების კორექტირება, როგორიცაა მოწყობილობის ბატარეის დარჩენილი ხანგრძლივობა და აპლიკაციის გადართვა. როდესაც მოწყობილობის ბატარეა განიმუხტება, უსაფრთხოების სქემის კონფიგურაცია სასურველია შემცირებული სირთულით, ნაკლები ენერგიის მოხმარებისთვის. ამ ორი საკითხის გათვალისწინებით,

უსაფრთხოების სქემების შერჩევა და კონფიგურაცია 6G ქსელში უნდა იყოს მორგებული ადაპტირებულად და დინამიკურად სხვადასხვა სცენარზე. იმავდროულად, ენერგოეფექტიანობა ხდება სულ უფრო კრიტიკული საკითხი 6G უსაფრთხოებაში. მოწყობილობებსა და საბაზო სადგურებს შეიძლება ჰქონდეთ შეზღუდული სიმძლავრე უსაფრთხოების სქემების განხორციელების მხარდასაჭერად მათი აპარატურული შესაძლებლობებისა და ფიზიკური მდებარეობის გამო. ენერგიის მაღალი მოხმარება ასევე ზრდის საოპერაციო ხარჯებს, რაც მთავარი ბარიერია 6G ქსელის სამომავლო კომერციალიზაციისთვის. 6G უსაფრთხოების გადაწყვეტილებების სირთულე უნდა იყოს მორგებული სხვადასხვა სცენარზე, ჰეტეროგენული ქსელებისა და დინამიკური ოპერაციული პირობების საპასუხოდ. ამიტომ, 6G უსაფრთხოება უნდა დარეგულირდეს ენერგოეფექტიანობის თვალსაზრისით და ამავე დროს უზრუნველყოფილი უნდა იყოს უსაფრთხოების სასურველი ხარისხი.

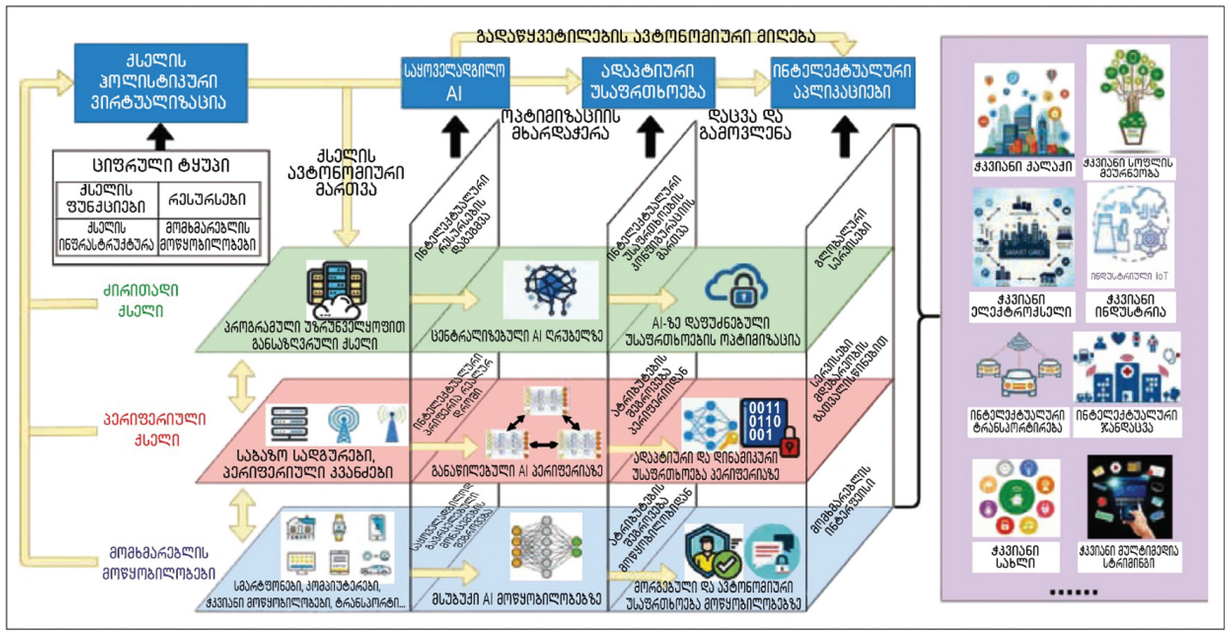
ამ თავში ჩვენ ვიკვლევთ ადაპტირებულ და დინამიკურ უსაფრთხოებას 6G ქსელში ენერგოეფექტიანობის პერსპექტივიდან, რათა დავაბალანსოთ უსაფრთხოებისა და ენერგეტიკის ურთიერთდამოკიდებულება სხვადასხვა სცენარში. კერძოდ, ჩვენ შევისწავლით AI-ზე დაფუძნებული 6G ქსელის არქიტექტურას და გამოვავლენთ პერსპექტიულ ინტელექტუალურ აპლიკაციებს. მეორე, ჩვენ განვიხილავთ უსაფრთხოების სტრატეგიის ოპტიმიზაციის გამოწვევებს, წარმოშობილი საფრთხეებისა და მათთან დაკავშირებული საკითხების იდენტიფიცირებით, უსაფრთხოებასა და ენერგეტიკას შორის ურთიერთდაბალანსებისას ჰეტეროგენულობის, დინამიკისა და მოდელირების სირთულის თვალსაზრისით. შემდეგ განვიხილავთ 6G უსაფრთხოების ოპტიმიზაციის სტრუქტურას, რომელიც აერთიანებს არაადიტიურ მაჩვენებლებზე დაფუძნებულ ატრიბუტების არჩევანს და კომპლექსური ფუნქციების აპროქსიმაციას, მოდელის ტრენინგისთვის. შემოთავაზებული სტრუქტურა უზრუნველყოფს უსაფრთხოების ადაპტირებულ და დინამიკურ გადაწყვეტილებებს სხვადასხვა სცენარისთვის, რათა შემცირდეს ენერგიის მოხმარება და გარანტირებული იყოს უსაფრთხოების სასურველი დონე. შემდეგ, ჩვენ განვიხილავთ რამდენიმე ღია საკითხს ენერგოეფექტიანობის თვალსაზრისით, 6G უსაფრთხოების ოპტიმიზაციის შესახებ.

ამ თავის დარჩენილი ნაწილი ორგანიზებულია შემდეგნაირად: მომდევნო პარაგრაფი გვთავაზობს 6G-ის არქიტექტურას, პერსპექტიულ აპლიკაციებს და ძირითად ხედვებს. ამის შემდეგ განიხილება 6G-ის უსაფრთხოების გამოწვევები და წარმოდგენილია ოპტიმიზაციის სტრუქტურა 6G-ის უსაფრთხოებისთვის. დაბოლოს, განიხილება კვლევების ღია საკითხები და მოცემულია დასკვნები.

4.2. 6G-ის არქიტექტურისა და ხედვების მიმოხილვა

ჩვენ წარმოვადგენთ AI-ზე დაფუძნებულ არქიტექტურას 6G ქსელისთვის, როგორც ნაჩვენებია ნახ. 4.1-ზე. 5G არქიტექტურასთან შედარებით, მოსალოდნელია, რომ 6G ქსელი გამოიყენებს AI მეთოდებს ყველგან, რათა მხარი დაუჭიროს ინტელექტუალურ სერვისებს ძირითად ქსელში, პერიფერიულ ქსელში და მომხმარებლის მოწყობილობებში:

- ძირითადი ქსელი შედგება SW-ით განსაზღვრული ქსელისაგან, ინტელექტუალური რესურსების დაგეგმვისა და უსაფრთხოების კონფიგურაციის მართვისთვის. ზუსტი კომპიუტერული სიმულაცია შეიძლება განხორციელდეს ვირტუალიზებულ ქსელურ ინფრასტრუქტურაზე ოპერატიული მონაცემების შესაგროვებლად და ქსელის მართვის სწორი სტრატეგიების დასადგენად. სიმულაციური მონაცემების მიხედვით, AI ძირითად ქსელში ახორციელებს ქსელის ავტონომიურ მართვას. ცენტრალიზებული AI ასევე გამოიყენება გლობალური სერვისებისთვის გადაწყვეტილების მისაღებად მოდელის ტრენინგის პარამეტრებისა და პერიფერიული ქსელიდან გადაცემული მონაცემების აგრეგაციის გზით.



ნახ. 4.1. შემოთავაზებული, AI-ზე დაფუძნებული 6G ქსელის არქიტექტურა

- AI შეიძლება განაწილდეს ცენტრალიზებული ღრუბლიდან 6G ქსელის პერიფერიამდე, როგორიცაა საბაზო სადგურები, ინტელექტუალურ პერიფერიაზე გამოთვლის, მობილურობისა და HO-ის მართვის, რესურსების ორკესტრირებისა და ამოცანების დაგეგმვისთვის. მონაცემთა სიმწირესთან და მომხმარებლის კონფიდენციალურობასთან დაკავშირებული საკითხების მოსაგვარებლად, ფედერირებული სწავლება შეიძლება გამოყენებულ იქნეს პერიფერიულ კვანძებზე, რათა ერთობლივად დაატრენინგოს განაწილებული AI მოდელები იმავე პრობლემის გადასაჭრელად, მოდელის პარამეტრების გაერთიანებით ძირითად ქსელში. AI-ზე დაფუძნებული პერიფერიული ქსელი უზრუნველყოფს ინტელექტუალურ სერვისებს უფრო დაბალი შეყოვნებით და მდებარეობის ინფორმირებულობით მომხმარებლის მოწყობილობებთან სიახლოვის გამო.
- მილიარდობით ჰეტეროგენული მომხმარებლის მოწყობილობა დაკავშირებულია 6G ქსელთან, როგორიცაა სმარტფონები, სენსორები და მანქანები გამოთვლების, შენახვისა და ენერგიის სხვადასხვა დონის შესაძლებლობებით. შეგროვებული მონაცემები და მომხმარებლის მოთხოვნები გადაეცემა პერიფერიულ ქსელში არსებულ საბაზო სადგურებს. მომხმარებლის მოწყობილობებზე ჩადგმული „მსუბუქი“ AI-ის მხარდაჭერით, ინტელექტუალური სერვისები შეიძლება განხორციელდეს უფრო ზუსტად, რეალურ დროში და უფრო რობასტულად, ვიდრე 5G ქსელებში.

AI-ით მხარდაჭერილი არქიტექტურის საფუძველზე, განვითარებადი ინტელექტუალური სერვისები შეიძლება დაინერგოს 6G ქსელში, რაც სარგებელს მოუტანს ყოველდღიურ ცხოვრებას, ინდუსტრიულ წარმოებას და ქალაქის მმართველობას. მაგალითად, სატრანსპორტო საშუალებების ინტერნეტი ისარგებლებს 6G-ის ფართო დაფარვით, რომელიც საშუალებას მისცემს მანქანებს, თვითმფრინავებს და გემებს, მიაღწიონ უწყვეტ კავშირს მოძრაობის უსაფრთხოებისა და მოგზაურობის ეფექტიანობის უზრუნველსაყოფად. მიუხედავად იმისა, რომ ინტელექტუალური ტრანსპორტი გარკვეულწილად უკვე ინერგება 5G ქსელებით, 6G ქსელი მნიშვნელოვნად გააფართოებს მანქანების დაკავშირების პროცესს ხმელეთიდან კოსმოსში, საჰაერო ხომალდებში და წყალქვეშა ზონებში. ბლოკჩეინზე დაფუძნებული

ტექნოლოგიების მეშვეობით ინფორმაციის გაცვლამ და მონაცემთა დამუშავებამ დაკავშირებულ მანქანებს შორის, შეიძლება უზრუნველყოს უკეთესი დეცენტრალიზაცია, უსაფრთხოება, გამჭვირვალობა, უცვლელობა და ავტომატიზაცია. მომდევნო ათწლეულში, სატრანსპორტო ინტერნეტი, სავარაუდოდ, გააერთიანებს ავტონომიური მართვის ტექნოლოგიებს, რაც ტრანსპორტირებას საშუალებას მისცემს, იყოს დამოუკიდებელი მომხმარებლის ჩარევისგან; ასე რომ შესაძლებელი გახდება ცხოვრების ახალი სტილი, როგორიცაა მობილური მუშაობა და მობილური გართობა. გარდა ამისა, ჭკვიანი ინდუსტრიის რეალიზება შესაძლებელია 6G-ში დანერგილი „ციფრული ტყუპის“ ტექნოლოგიით, რომელიც კიბერსივრცეში ფიზიკური წარმოების გარემოს ვირტუალურ ასლს ქმნის. საქარხნო წარმოების ჯაჭვის „ციფრული ტყუპი“ მოიცავს ვირტუალიზებულ მუშაკებს, მანქანებს, ნედლეულს და პროდუქტის მთელ სასიცოცხლო ციკლს. წარმოების ისტორიულ მონაცემებზე დაყრდნობით, ჭკვიანი ინდუსტრია რეალურ დროში ახორციელებს მონიტორინგს და წარმოების პოლიტიკის ოპტიმიზაციას, რათა წარმოების ჯაჭვის ყველა ელემენტმა შეძლოს მათი ქმედებების კოორდინაცია მაქსიმალური ეფექტიანობით. გარდა ამისა, ყველგან გავრცელებული 6G ჭკვიანი ქსელით, უფრო მეტი საჯარო სერვისის რეალიზება შეიძლება ჭკვიანი ქალაქისთვის. მილიარდობით ინტელექტუალური მოწყობილობით, რომელიც მუშაობს კოსმოსში, ჰაერში, ხმელეთსა და ოკეანეში, საჯარო სერვისებს შეუძლიათ გადალახონ გეოგრაფიული დაბრკოლებები, რათა მიაღწიონ საჯარო რესურსების დაბალანსებულ განაწილებას, როგორიცაა დისტანციური სამედიცინო მკურნალობა და დისტანციური განათლება. AI-ზე დაფუძნებული არქიტექტურისა და პერსპექტიული ინტელექტუალური აპლიკაციების რეალიზებისთვის, 6G ქსელი უნდა იყოს უფრო მეტი, ვიდრე უბრალოდ 5G-ის მოწინავე ვერსია და მოსალოდნელია ზოგიერთი რევოლუციური წინსვლა, როგორც ხედვა 6G-სთვის.

ახლა განვიხილოთ AI-სთან დაკავშირებული ძირითადი ხედვები.

ყოვლისმომცველი AI: 6G ქსელში, მოსალოდნელია ინტელექტის დეცენტრალიზება და განაწილება პერიფერიაზე (მაგალითად, საბაზო სადგურებზე) და მომხმარებლის მოწყობილობებზე, დიდი მონაცემების ხელმისაწვდომობისა და გამოთვლითი შესაძლებლობების მნიშვნელოვანი განვითარების გამო. IoT-ის განვითარებით, 5G ქსელები აკავშირებს უამრავ ჭკვიან მოწყობილობას, რათა გააუმჯობესოს ადამიანი-ადამიანი და ადამიანი-საგანი კომუნიკაციის ხარისხი, რაც იძლევა ინფორმაციის წვდომისა და გაზიარების საშუალებას ყველგან, ნებისმიერ დროს. ინფორმაციის ყოვლისმომცველობაზე დაყრდნობით, 6G ქსელი შექმნილია საყოველთაო ინტელექტის მისაღწევად, რათა უზრუნველყოს ინტელექტუალური აპლიკაციების სიმრავლე და ქსელის ავტონომიური მენეჯმენტი გადაწყვეტილებების მიღებისას, ადამიანის შემცირებული ჩარევით. საჭიროა ყოვლისმომცველი AI, რადგან 6G სცენარების უმეტესობა მრავალფეროვანი და დინამიკურია, მოითხოვს შაბლონის სწავლებას და დაბალ შეყოვნებას სწრაფი პასუხების უზრუნველსაყოფად. მაგალითად, სრულად ავტონომიური მართვის განსახორციელებლად, თითოეულმა მანქანამ უნდა შეისწავლოს მართვის საკუთარი შაბლონი მანქანის სტატუსის, მომხმარებლის პრეფერენციების მიხედვით და მიიღოს რეალურ დროში მართვის გადაწყვეტილებები რთული სატრანსპორტო გარემოს საპასუხოდ. ღრუბელში ცენტრალიზებული ჩვეულებრივი AI ვეღარ აკმაყოფილებს 6G სერვისების მოთხოვნებს. მოსალოდნელია, რომ დეცენტრალიზებული AI-ის მეთოდები, განსაკუთრებით პერიფერიული მოწყობილობებით მიღებული ინტელექტი, მნიშვნელოვან როლს შეასრულებს 6G ქსელში. ფედერირებული სწავლება შეიძლება განხორციელდეს პერიფერიული ინტელექტის გასაუმჯობესებლად, ტრენინგის მონაცემების დაუბალანსებელი განაწილების პრობლემის გადასაჭრელად. ლოკალური AI მოდელები პერიფერიულ კვანძებში შეიძლება ერთობლივად იქნან დატრენინგებული ფედერირებული სწავლების მეშვეობით გლობალური ცოდნის აღმოჩენის მისაღწევად.

ქსელის ჰოლისტიკური ვირტუალიზაცია: ხელოვნური ინტელექტის ფართოდ გავრცელებით, 6G ქსელის მენეჯმენტი, სავარაუდოდ, უზრუნველყოფს უფრო ინტელექტუალური ამოცანების დაგეგმვასა და რესურსების მართვას, ვიდრე წინა თაობები. 5G-ში ვირტუალიზაცია ოპტიმიზაციას უკეთებს რესურსების განაწილებას ისეთი ფუნქციების დანერგვით, როგორიცაა დატვირთვის დაბალანსება, მარშრუტირება და უსაფრთხოების გადაწყვეტილებები, როგორც პროგრამული ინსტანციები, რომლებიც მუშაობენ ვირტუალურ მანქანებზე. 6G ქსელი შექმნილია ვირტუალიზაციისა და SW-ის ფარგლების გაფართოებისთვის, რათა მოიცვას ქსელის ინფრასტრუქტურა, მომხმარებლის მოწყობილობები, ქსელის რესურსები და შესაბამისად განხორციელდეს ქსელის ჰოლისტიკური ვირტუალიზაცია (HNV). ამ პირობებში შეიქმნება მომხმარებლის მოწყობილობებისა და საბაზო სადგურების ციფრული ასლები შესაბამისი აპარატურის წარმოსაჩენად. HNV უზრუნველყოფს მთელი ქსელის ინფრასტრუქტურის და მრავალი მომხმარებლის მოწყობილობის მძლავრ სიმულაციას ქსელის მართვისა და რესურსების ორკესტრირების სხვადასხვა სტრატეგიის შესაფასებლად. HNV სიმულაციების მიერ გენერირებული ზუსტი და ყოვლისმომცველი მონაცემების შესწავლით, 6G-ში გავრცელებულ AI-ის შეუძლია ავტომატურად განსაზღვროს ქსელის მართვის სტრატეგიები. შემდეგ HNV სინქრონიზებს ქსელის ინფრასტრუქტურისა და მომხმარებლის მოწყობილობების სხვადასხვა კონფიგურაციას ფიზიკურ ობიექტებთან, ქსელის მუშაობის ოპტიმიზაციისთვის, როგორიცაა შეყოვნება და ენერგოეფექტიანობა. ამიტომ, HNV განიხილება, როგორც მნიშვნელოვანი 6G ხედვა ქსელის ავტონომიური მართვისთვის.

4.3. გამოწვევები 6G-ის უსაფრთხოების კუთხით

ზემოაღნიშნული ხედვების გარდა, ადაპტიური უსაფრთხოება ასევე მნიშვნელოვანი მოლოდინია 6G ქსელისთვის. მიუხედავად იმისა, რომ 5G-ში მოგვარდა უსაფრთხოების მრავალი დაუცველობა, როგორიცაა საკომუნიკაციო არხების უკანონო თვალთვალი, კომპრომეტირებული წვდომის წერტილები, კონფიდენციალურობის გაჟონვა და პირადობის გაყალბება, 6G უსაფრთხოება ახალი გამოწვევების წინაშე დგას. პირველ რიგში, 6G-ში არსებული SW-ის და ქსელური ინტელექტის გამო, ჩნდება ახალი საფრთხეები, რომლებიც მიმართულია ხელოვნური ინტელექტის ტრენინგის პროცესზე. უფრო მძლავრი უსაფრთხოების გადაწყვეტილებებია საჭირო AI-სთან დაკავშირებული ახალი საფრთხეების დასაძლევად, როგორიცაა ბექდორის (backdoor) ჩაშენება და ტრენინგის მონაცემების მოწამვლა ფედერირებულ სწავლებაში. მეორეც, 5G ქსელებს არ გააჩნია უნივერსალური სტანდარტი უსაფრთხოების სტრატეგიის ოპტიმიზაციისთვის სხვადასხვა სცენარში, რათა დააკმაყოფილოს უსაფრთხოების სხვადასხვა მოთხოვნა და შემცირდეს შესაბამისი ოვერჰედები. მაგალითად, როდესაც მოწყობილობის დარჩენილი ბატარეა იწურება, გამოყენებული უსაფრთხოების სქემების სირთულე უნდა დარეგულირდეს მოწყობილობის მუშაობის დროის გასაზრდელად. 6G ქსელის ჰეტეროგენულობის, დინამიკისა და სირთულის ზრდასთან ერთად, უსაფრთხოება უნდა იყოს ადაპტიურად კონფიგურირებადი სხვადასხვა ტიპის სერვისთვის, ენერგიის მოხმარების პირობებისთვის და დროში ცვალებადი სხვა ატრიბუტებისთვის. ამ პარაგრაფში, ჩვენ ჯერ განვსაზღვრავთ საფრთხეებს 6G ქსელში და შემდეგ განვიხილავთ უსაფრთხოების საკითხებს, გამომდინარე ენერგოეფექტიანობის პერსპექტივიდან.

4.3.1. წარმოქმნილი საფრთხეები

ბევრი ტრადიციული საფრთხე 6G-ში, როგორიცაა DDoS, მავნე პროგრამების ინექცია და გვერდითი არხიდან თავდასხმები, მომდინარეობს წინა თაობებიდან. იმავდროულად, AI-ის ყოვლისმომცველი გა-

ვრცელება ზრდის 6G ქსელის დაუცველობას ახალი საფრთხეების მიმართ, რომლებიც აზიანებს AI-ის ხელმისაწვდომობასა და მთლიანობას.

AI-ის ხელმისაწვდომობის საფრთხეები: ისინი ხელს უშლიან მომხმარებლებს. გამოიყენონ ინტელექტუალური სერვისები და ქსელის ავტონომიური მენეჯმენტი, ახორციელებენ რა თავდასხმას ინტელექტუალური მონაცემების ხელმისაწვდომობაზე, რომელიც განაწილებულია პერიფერიულ ქსელში და მომხმარებლის მოწყობილობებზე. შედეგად, ზოგჯერ AI-ის პროცესები პერიფერიულ კვანძებსა და მოწყობილობებში დაზიანებულია ისე, რომ DL მოდელების მიერ გონივრული გადაწყვეტილებების მიღება შეუძლებელია. მაგალითად, მოწამვლის თავდასხმას შეჰყავს გაყალბებული მონაცემები მომხმარებლის მოდელის სასწავლო აუზში, რათა გადაიტანოს მოდელის გადაწყვეტილების საზღვრები, რაც იწვევს არაგონივრულ გადაწყვეტილებებს ან არაზუსტ პროგნოზს. შეყვანილი მონაცემები დეტალურად არის გაყალბებული სამიზნე სერვისის მონაცემთა განაწილების მიხედვით, ასე რომ, ინექციის მცირე ნაწილმაც კი შეიძლება მოწამლოს ტრენინგის მონაცემთა მთელი ნაკრები და სიზუსტის მნიშვნელოვანი დაქვეითება გამოიწვიოს. ვინაიდან, ამ დროს DL მოდელი ნორმალურად ვერ ფუნქციონირებს, AI-ის ხელმისაწვდომობა თავდამსხმელების მიერ ზიანდება.

AI-ის მთლიანობის საფრთხეები: ეს არ აზიანებს AI-ის ხელმისაწვდომობას, მაგრამ ტოვებს კომპრომეტირებულ AI-ის, თითქოსდა ნორმალურად ფუნქციონირებისთვის. იმის მაგივრად, რომ მოახდინოს ფალსიფიცირებული ტრენინგის მონაცემების ინექცია, თავდამსხმელები მოდელში ახდენენ ბექდორის სიგნალების შეყვანას მომხმარებლის ინფორმირებულობის გარეშე. ბექდორის ტრიგერის შეყვანით, როგორიცაა გარკვეული სტრიქონი ფაილში ან პიქსელის შაბლონი გამოსახულებაში, თავდამსხმელებს შეუძლიათ გამოიყენონ კომპრომეტირებული მოდელი, რათა უზრუნველყონ სასურველი კლასიფიკაცია ან გამოვლენის შედეგები, მიუხედავად რეალური მონაცემების შეყვანისა. 5G-სთან შედარებით, მოსალოდნელია, რომ 6G ქსელი უფრო დაუცველი იქნება ბექდორზე დაფუძნებული თავდასხმების მიმართ, მოწინავე AI ტექნიკის პოპულარობის გამო, როგორიცაა ტრანსფერული და ფედერირებული სწავლება. მაგალითად, ტრანსფერული სწავლება მომხმარებლებს ეხმარება გადაჭრან საკუთარი პრობლემები შეზღუდული DB-ის გამოყენებისას, რადგან მომხმარებლები იყენებენ წინასწარ დატრენინგებულ მოდელს (რომელიც შექმნილია შესაბამისი პრობლემის მიხედვით), რათა დახვეწონ საკუთარი მოდელები. თუ მესამე მხარის მიერ მოწოდებული წინასწარ დატრენინგებული მოდელი ჩასმულია ბექდორიდან, მთელი სწავლების პროცესი შეიძლება დაზარალდეს.

AI-სთან დაკავშირებული თავდასხმის დაწყებისას, როგორიცაა მონაცემთა მოწამვლის თავდასხმა ან შეჯიბრებითი სწავლება, თავდამსხმელები ჯერ პოულობენ წვდომას AI სისტემების ტრენინგის DB-ზე. ბევრი აპლიკაცია აგროვებს ტრენინგის მონაცემებს საჯარო მომხმარებლებისგან, რათა გააუმჯობესოს მათი DL მოდელები, როგორიცაა სპამის ელექტრონული ფოსტის ფილტრები. ამ აპლიკაციებს აქვთ მაღალი დაუცველობა AI-ის კუთხით თავდასხმების მიმართ, რადგან ისინი ძნელად ამოწმებენ მომხმარებლების შემავალი მონაცემების საიმედოობას. ტრენინგის DB-ზე წვდომის მიღების შემდეგ, თავდამსხმელებს აქვთ მრავალი საშუალება, რათა დაარღვიონ გენერირებული AI მოდელის ნორმალური ფუნქციონირება. მონაცემთა მოწამვლა და ბექდორის ინსტალაცია, როგორც უკვე განვიხილეთ, დატრენინგებული კლასიფიკატორის რეგულირების ორი ჩვეულებრივი გზაა, რათა უზრუნველყოს ცრუ შედეგი მისი გადაწყვეტილების საზღვრებში ჩარევით. მაგალითად, ავტონომიური მართვისას, მანქანებმა უნდა ამოიცნონ გაჩერების ნიშნები გზისპირა სურათების გამოყენებით, ტრენინგის მონაცემთა ნაკრებიდან საერთო გაჩერების ნიშნების გამოსახულების შაბლონების შესწავლით. თუ თავდამსხმელები ახდენენ გაჩერების ნიშნების დიდი რაოდენობით ინექციას ტრენინგის DB-ში და ასახელებენ მათ, როგორც მწვანე შუქნიშანს, ავტომობილის კლასიფიკატორმა შეიძლება დააკავშიროს გაჩერების

ნიშნების შაბლონები მწვანე შუქნიშანთან, ასე რომ, ის განაგრძობს მოძრაობას გზაჯვარედინზე. ამ მიზნით, AI-სთან დაკავშირებულმა თავდასხმებმა შეიძლება სერიოზული ზიანი მიაყენოს მომხმარებლის უსაფრთხოებას 6G ქსელში AI აპლიკაციების საყოველთაო სიმრავლის გამო. ჩვეულებრივი და AI-სთან დაკავშირებული საფრთხეების მოსაგვარებლად, ადეკვატური უსაფრთხოება გარანტირებული უნდა იყოს მილიარდობით დაკავშირებულ მოწყობილობასა და მილიონობით საბაზო სადგურზე, სადაც ენერგიის მაღალი მოხმარება მთავარ დაბრკოლებად იქცევა.

4.3.2. უსაფრთხოების საკითხები ენერგეტიკული თვალსაზრისით

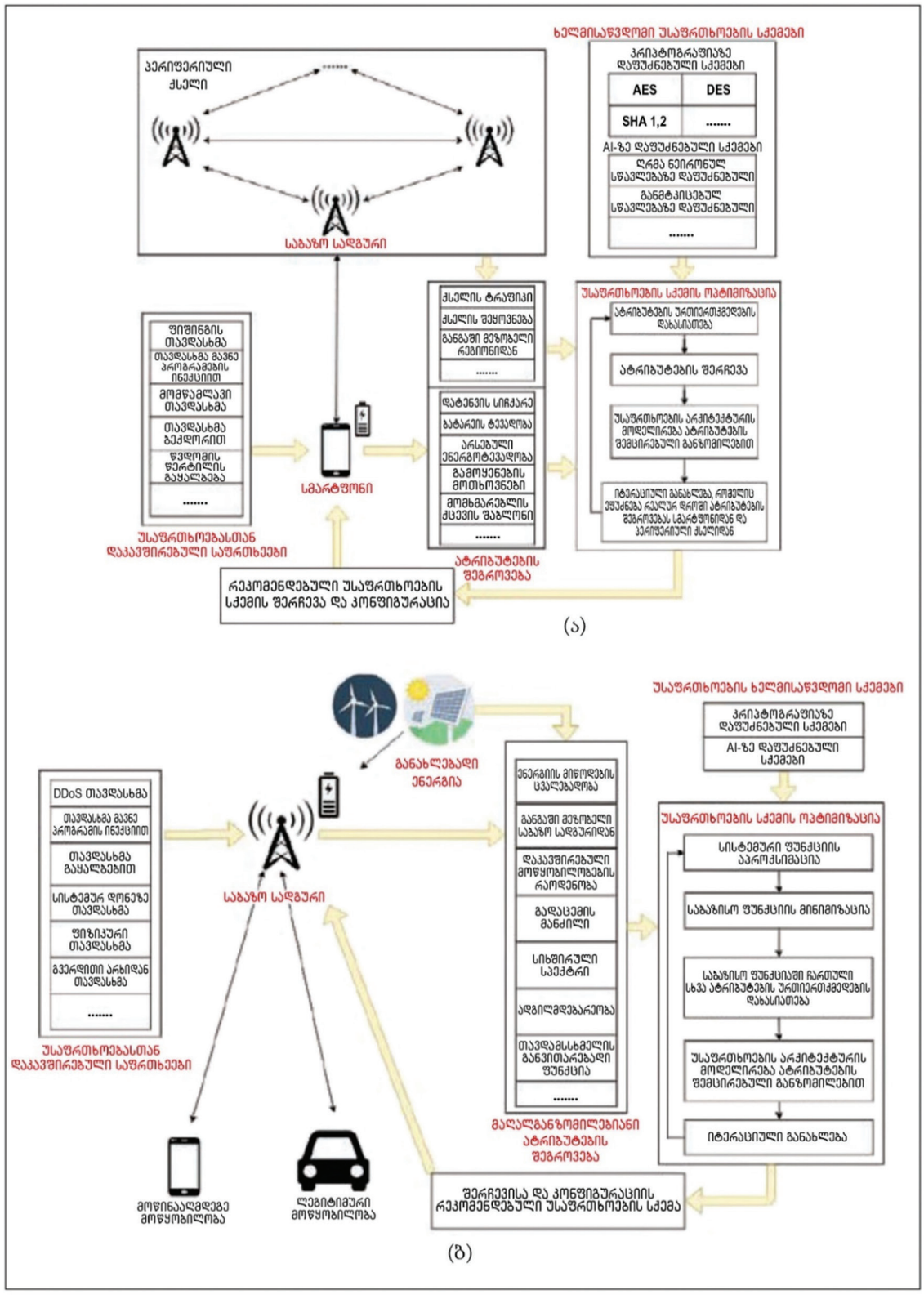
წინა თაობებთან შედარებით, 6G ქსელში ენერგოეფექტიანობის მოთხოვნას უფრო მეტი პრიორიტეტი ენიჭება, რათა გათვალისწინებულ იქნეს შეზღუდული სიმძლავრის მქონე მოწყობილობების დიდი რაოდენობა და განახლებადი ენერგიის წყაროებიდან ელექტრომომარაგების ცვალებადობა. სმარტფონისა და საბაზო სადგურის ორი შემთხვევა წარმოდგენილია ნახ. 4.2-ზე, როგორც მაგალითები, რომლებიც ასახავს 6G-ის უსაფრთხოების სტრატეგიის ოპტიმიზაციას უსაფრთხოებასა და ენერგიის მოხმარებას შორის კომპრომისის დასაბალანსებლად.

კომპრომისი უსაფრთხოებასა და ენერგიის მოხმარებას შორის: მომხმარებლებს შეუძლიათ დააბალანსონ უსაფრთხოებასა და ენერგეტიკას შორის კომპრომისი უსაფრთხოების სხვადასხვა სქემის შერჩევით და მათი კონფიგურაციების მორგებით სხვადასხვა მოწყობილობის შესაძლებლობების, ენერგეტიკული პირობების, თავდასხმისას დაუცველობის, სერვისებისა და სხვა ატრიბუტების მიხედვით. ამ თავში განვიხილავთ უსაფრთხოების არსებული სქემების ორ ძირითად კატეგორიას: კრიპტოგრაფიაზე და AI-ზე დაფუძნებულ სქემებს. პირველი კატეგორია იყენებს კრიპტოგრაფიულ გასაღებებს უსაფრთხოების დაცვის ამოცანებისთვის, მათ შორის მონაცემთა დაშიფვრის, ავთენტიფიკაციისა და ციფრული ხელმოწერების ჩათვლით. სხვადასხვა ალგორითმის არჩევით, როგორიცაა AES, მონაცემთა შიფრირების სტანდარტი (DES), რივესტ-შიფრატორი 4 (RC4) და უსაფრთხო ჰეშირების ალგორითმები (SHA) და მათი გასაღებების სიგრძეების რეგულირებით, მომხმარებლებს შეუძლიათ შეცვალონ უსაფრთხოების სიძლიერე და ენერგიის მოხმარება სხვადასხვა სცენარისთვის. მეორე კატეგორიის სქემები უფლებამოსილია AI-ის მიერ, რათა აღმოაჩინონ მავნე ქცევები, თავდამსხმელის შეჭრა და სისტემის არანორმალური სტატუსი. სხვადასხვა AI ტექნიკა, როგორიცაა DNN, RL და დამხმარე ვექტორული მანქანა (SVM), გამოიყენება უსაფრთხოების არსებული სქემების შესაქმნელად. AI-ით მართვადი ეს სქემები, როგორც წესი, მოიხმარენ დიდი რაოდენობით გამოთვლით სიმძლავრეს და ენერგიას ძირითადი აპარატურისგან. ვინაიდან ჩაშენებული მოწყობილობები და პერიფერიული მიკროკვანძები ფართოდ არის განლაგებული 6G ქსელში მრავალფეროვანი თვისებებითა და რესურსების შეზღუდვით, AI-ზე დაფუძნებული სქემების ერთობლიობა ასევე უნდა იყოს კონფიგურირებადი. მაგალითად, მოდელის ტრენინგის დროს უნდა განისაზღვროს სხვადასხვა კონფიგურაცია, როგორიცაა მოდელის სტრუქტურა, ტრენინგის ალგორითმი და ტერმინალური პირობები, რათა ვიპოვოთ საუკეთესო შესაძლო კომპრომისი უსაფრთხოებასა და ენერგიის მოხმარებას შორის.

უსაფრთხოებასა და ენერგეტიკას შორის კომპრომისის დაბალანსება: 6G-ში უსაფრთხოებასა და ენერგეტიკას შორის ოპტიმალური კომპრომისის მიღწევა შეიძლება ბევრად უფრო რთული იყოს, ვიდრე 5G-ში, მნიშვნელოვნად გაზრდილი ჰეტეროგენულობის, დინამიკის და მოდელის შექმნის სირთულის გამო.

ჰეტეროგენულობა: ვინაიდან 6G ქსელი აკავშირებს უზარმაზარი მოცულობის მოწყობილობებსა და საბაზო სადგურებს სხვადასხვა შესაძლებლობითა და სამუშაო პირობებით, 5G-ის ერთიანი სტრატეგია აღარ არის შესაფერისი 6G უსაფრთხოებისთვის. ჰეტეროგენულობა სრულად უნდა იქნეს გათვალისწინებული ენერგოეფექტიანი უსაფრთხოების ოპტიმალური სქემის დასადგენად. 6G ქსელი შეიცავს ჰეტე-

როგენულ სერვისულ მახასიათებლებს, ტექნიკურ შესაძლებლობებს, კომუნიკაციის პირობებს, ელექტრომომარაგებასა და თავდასხმის ტიპებს, რაც იწვევს უსაფრთხოებისა და ენერგიის ხელმისაწვდომობის უაღრესად მრავალფეროვან მოთხოვნებს. უსაფრთხოებასა და ენერგეტიკას შორის კომპრომისის დაბალანსების პროცესი უნდა იყოს ადაპტირებული ჰეტეროგენულ 6G ქსელთან.



ნახ. 4.2. უსაფრთხოების ადაპტიური და დინამიკური ოპტიმიზაციის სცენარები: ა) მომხმარებლის მოწყობილობისთვის; ბ) საბაზო სადგურისთვის

დინამიკა: 6G ქსელის დროში ცვალებადი ბუნება ართულებს კომპრომისს უსაფრთხოებასა და ენერგეტიკას შორის უსაფრთხოების მოთხოვნებისა და ენერგიის ხელმისაწვდომობის განსხვავების გამო. დროდადრო შეიძლება მოხდეს ქსელის სტატუსის ვარიაციები, როგორიცაა მნიშვნელოვანი ცვლილებები გადაცემის ტრაფიკში ან შეყოვნებაში, აგრეთვე მეზობელი საბაზო სადგურების ან მოწყობილობების მიერ მოწოდებული თავდასხმის შესახებ გაფრთხილებები. დროში ცვალებადია ელექტრომომარაგების მდგომარეობაც: ისეთი მოწყობილობებისთვის, როგორიცაა სმარტფონები, ბატარეას შეიძლება ჰქონდეს დაბალი ტევადობა, ამიტომ მძლავრი უსაფრთხოების სქემები შეიძლება შეიზღუდოს უფრო ხანგრძლივი მუშაობის დროით; საბაზო სადგურებისთვის განახლებადი ენერგიის წყაროებს, როგორიცაა ქარის და მზის ენერგია, ასევე აქვთ მიწოდების რყევები. ამრიგად, უსაფრთხოების სქემების შერჩევა და კონფიგურაცია უნდა განახლდეს იტერაციულად, რათა მოგვარდეს დინამიკა 6G ქსელში.

მოდელირების სირთულე: ატრიბუტების დიდი რაოდენობა, როგორც ნაჩვენებია ნახ. 4.2-ზე, შეიძლება მომდინარეობდეს სერვისის მახასიათებლების, აპარატურული შესაძლებლობების, ქსელის მუშაობის პირობების, ენერგიის სტატუსისა და თავდასხმიდან დაუცველობის ასპექტებიდან. მრავალრიცხოვან ატრიბუტებსა და სასურველ უსაფრთხოების სტრატეგიას შორის ურთიერთობის მოდელირება შეიძლება საკმაოდ რთული იყოს უსაფრთხოებასა და ენერგეტიკას შორის კომპრომისის დასაბალანსებლად. უსაფრთხოების ოპტიმიზაციის მოდელირების პროცესი უნდა იყოს „მსუბუქი“ – ისე, რომ დამატებითი ოვერჰედი არ ეწინააღმდეგებოდეს ენერგოეფექტიანობის სარგებლიანობას, რომელიც მიღწეულია 6G უსაფრთხოების სტრუქტურით. ამიტომ, მოდელირების სირთულის შემცირება კრიტიკული გამოწვევაა 6G უსაფრთხოების ოპტიმიზაციისთვის.

ამ გამოწვევების გადასაჭრელად, უსაფრთხოებასა და ენერგეტიკას შორის კომპრომისის დაბალანსების კუთხით, ჩვენ განვიხილავთ დინამიკური და „მსუბუქი“ ოპტიმიზაციის სტრუქტურას ადაპტიური უსაფრთხოებისთვის 6G ქსელში.

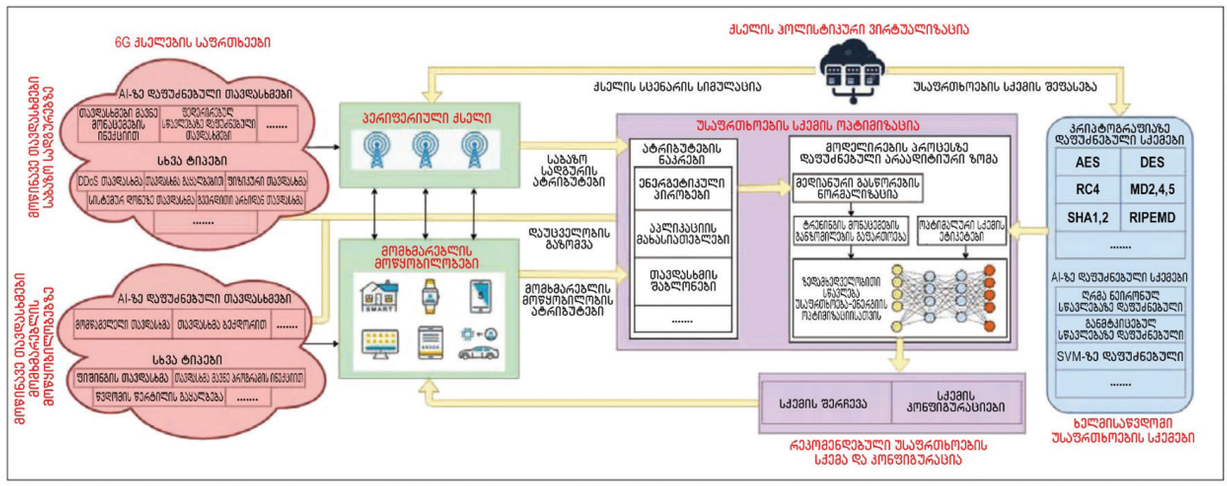
4.4. ოპტიმიზაციის სტრუქტურა უსაფრთხოებასა და ენერგეტიკას შორის კომპრომისისთვის

4.4.1. შემოთავაზებული სტრუქტურის მიმოხილვა

შემოთავაზებულ ოპტიმიზაციის სტრუქტურას აქვს დიზაინის სამი პრინციპი: პირველი, გენერირებული ოპტიმიზაციის მოდელი უნდა იყოს ადაპტირებული სხვადასხვა სცენართან პერიფერიულ ქსელში და მომხმარებლის მოწყობილობებთან, რათა უსაფრთხოების სქემა შემუშავებული იყოს კონკრეტული საბაზო სადგურისთვის ან მოწყობილობისთვის, ენერგოეფექტიანობის თვალსაზრისით; მეორე, სტრუქტურამ უნდა გაითვალისწინოს 6G ქსელის დინამიკა ოპტიმიზაციის მოდელის იტერაციული განახლებით და რეალურ დროში უსაფრთხოების სქემის შერჩევისა და კონფიგურაციის რეკომენდაციების მიწოდებით; მესამე, სტრუქტურა უნდა იყოს მსუბუქი, რათა არ გამოიწვიოს ზედმეტი ხარჯები და ენერგიის მოხმარება 6G უსაფრთხოებისთვის. შემოთავაზებული სტრუქტურის მიმოხილვა ნაჩვენებია ნახ. 4.3-ზე.

ატრიბუტები გროვდება პერიფერიული ქსელიდან, მომხმარებლის მოწყობილობებიდან და უსაფრთხოების საფრთხეებიდან, ქსელის სტატუსის, მოწყობილობის/საბაზო სადგურის სტატუსის, ენერგიის სტატუსის და სხვა ინფორმაციის მითითებისთვის. HNV-ს შეუძლია უზრუნველყოს ტრენინგის საკმარისი მონაცემები შემოთავაზებული სტრუქტურისთვის, ქსელის სხვადასხვა სცენარის ზუსტი სიმულაციის მეშვეობით. სიმულაციურ ქსელში თავდასხმების პროაქტიული დანერგვით, უსაფრთხოების

სხვადასხვა სქემა და მისი კონფიგურაციები შეიძლება შეფასდეს ისეთი მეტრიკებით, როგორიცაა დაშიფვრის სიძლიერე, გამოვლენის სიხშირე და ენერგიის მოხმარება. შემდეგ შეიძლება განისაზღვროს უსაფრთხოების ოპტიმალური სქემა, რათა დააბალანსოს უსაფრთხოებასა და ენერგეტიკას შორის კომპრომისი, ენერგოეფექტიანობის შესახებ მომხმარებლის წინასწარ განსაზღვრული მოთხოვნების გათვალისწინებით. მაგალითად, მომხმარებელს შეუძლია მოითხოვოს უსაფრთხოების სქემის CPU-ის გამოყენება ერთ პროცენტზე ნაკლები, თუ დარჩენილი ენერგეტიკული ტევადობა არის b და c პროცენტებს შორის, რათა მომხმარებლის მოთხოვნები ჩამოყალიბდეს უბან-უბან განსაზღვრულ (piecewise) ფუნქციებად. ცხრილი 4.1 გვიჩვენებს ტრენინგის ნიმუშის მაგალითს, რომელიც მოიცავს შეგროვებულ ატრიბუტებს და შესაბამის უსაფრთხოების სტრატეგიებს, რომლებიც მიღებულია ქსელის სიმულაციისგან შემდგომი მოდელირების პროცესისთვის.



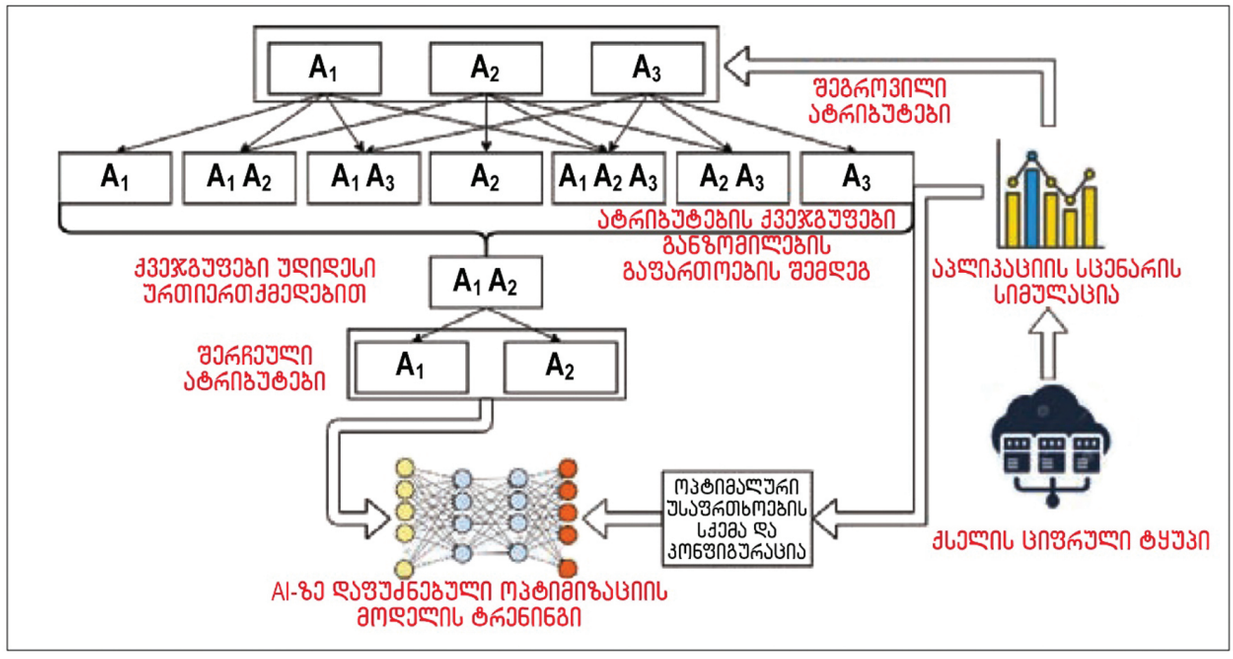
ნახ. 4.3. *შემოთავაზებული ოპტიმიზაციის სტრუქტურა უსაფრთხოების სქემის კონფიგურაციისთვის, დაბალანსებული კომპრომისით უსაფრთხოებასა და ენერგეტიკას შორის*

შემოთავაზებული AI-ზე დაფუძნებული სტრუქტურა მოიცავს ყველა დაკავშირებულ ატრიბუტს, როგორც ტრენინგის მონაცემებს, სწავლობს მათ ურთიერთობას სქემისა და კონფიგურაციის რეკომენდებულ არჩევანთან, რაც იწვევს მოდელირების მაღალ სირთულეს. ვინაიდან 6G უსაფრთხოების ოპტიმიზაცია მიზნად ისახავს ენერგოეფექტიანი უსაფრთხოების მიღწევას, აუცილებელია მოდელირების პროცესით გამოწვეული ენერგიის დამატებითი მოხმარების შეზღუდვა. არაადიტიურ მაჩვენებლებზე დაფუძნებული მოდელირების მიდგომა შემოთავაზებულია გამოთვლითი სირთულის შესამცირებლად. ამასთან, გენერირებული ოპტიმიზაციის მოდელის სიზუსტე გარანტირებულია. ოპტიმიზაციის შედეგის განსაზღვრისას, ატრიბუტებს შორის ურთიერთქმედების დახასიათებით, შემოთავაზებული მოდელირების მიდგომა ირჩევს მნიშვნელოვან ატრიბუტებს შემდგომი ზედამხედველობითი სწავლებისთვის ოპტიმიზაციის მოდელის შესაქმნელად. როგორც ნაჩვენებია ნახ. 4.4-ზე, სიმულაციისგან შეგროვებული ატრიბუტები გაფართოვდა ორიგინალური ატრიბუტების ნაკრების სიმძლავრის კომპლექტში. ატრიბუტების თითოეული ქვეჯგუფის ურთიერთქმედება იზომება ოპტიმიზაციის შედეგებზე ქვეჯგუფის ელემენტების კუმულაციური ეფექტის საჩვენებლად. უფრო დიდი ურთიერთქმედება გულისხმობს ქვეჯგუფის მიერ შეტანილ უფრო დიდ წვლილს უსაფრთხოებასა და ენერგეტიკას შორის კომპრომისის დაბალანსებაში. მხოლოდ ატრიბუტები, რომლებიც მიეკუთვნება ყველაზე დიდი ურთიერთქმედების მქონე ქვეჯგუფს, შეირჩევა AI-ზე დაფუძნებული ოპტიმიზაციის მოდელის ტრენინგისთვის, რათა მოდელის სირთულე არსებითად შემცირდეს. HNV-ზე დაფუძნებული სიმულაციის

მიერ მოწოდებული ტრენინგის მონაცემებით ოპტიმიზაციის მოდელის გენერირების შემდეგ, შემოთავაზებული სტრუქტურა იტერაციულად იძლევა რეალურ დროში უსაფრთხოების სქემის შერჩევისა და კონფიგურაციის რეკომენდაციას. ამ მიზნით, 6G ქსელის სხვადასხვა მოწყობილობასა და საბაზო სადგურებს შეუძლიათ შეცვალონ თავიანთი უსაფრთხოების სქემები უსაფრთხოებასა და ენერგეტიკას შორის ოპტიმალური ბალანსის მისაღწევად, მომხმარებლის მოთხოვნების შესაბამისად.

შერჩეული ატრიბუტები	მნიშვნელობა
აპლიკაცია	ონლაინ ბანკინგი
AI-ის გამოყენება	ბიომეტრიული იდენტიფიკაცია
ბატარეის ტევადობა	6400 მილიამპერი/სთ
დარჩენილი ტევადობა	80%
დატენვის სიჩქარე	65 ვატი
დატენილია თუ არა	არა
ნაკადების რაოდენობა	6
ადგილმდებარეობა	ურბანული
თავდასხმის ტიპი	DDoS
მეზობლების თავდასხმების რაოდენობის რაოდენობა	3
ქსელის შეყოვნება	700 მილიწმ
ქსელის ტრაფიკი	1000 მეგაბიტი/წმ
. . .	. . .
უსაფრთხოების სტრატეგია	კონფიგურაცია
კრიპტოგრაფიაზე დაფუძნებული სქემა	AES
კრიპტოგრაფიული გასაღების სიგრძე	1024 ბიტი
. . .	. . .

ცხრილი 4.1. შეგროვებული ატრიბუტების მაგალითი და უსაფრთხოების სტრატეგია, რომელიც გამოიყენება, როგორც ტრენინგის მონაცემები ოპტიმიზაციის ჩარჩოში



ნახ. 4.4. არაადიტიურ მაჩვენებლებზე დაფუძნებული მოდელირების პროცესი ოპტიმიზაციის მოდელისთვის

4.4.2. უსაფრთხოების ოპტიმიზაცია სხვადასხვა სცენარისთვის

AI-ზე დაფუძნებული ოპტიმიზაციის სტრუქტურა ახდენს ურთიერთობის მოდელირებას შეგროვებულ ატრიბუტებსა და უსაფრთხოების სქემებისთვის რეკომენდებულ არჩევანსა და კონფიგურაციებს შორის. უსაფრთხოებასა და ენერგეტიკას შორის კომპრომისი სხვადასხვა სცენარისთვის დაბალანსებულია ადაპტიური და დინამიკური გზით. მაგალითად, HW-ის შესაძლებლობებმა გამოთვლითი ტექნიკისა და კომუნიკაციის კუთხით, შეიძლება ასევე იმოქმედოს უსაფრთხოების ოპტიმიზაციაზე, ვინაიდან უსაფრთხოების სქემით გამოწვეული დამატებითი ოვერჰედი და შეყოვნება უნდა იყოს შეზღუდული. ელექტრომომარაგების სხვადასხვა ტიპი, როგორიცაა: სადენიანი დამუხტვა, უსადენო დამუხტვა და განახლებადი ენერგია, უზრუნველყოფს სხვადასხვა ენერგეტიკულ სიმძლავრეებს და დატენვის სიჩქარეს მომხმარებლის მოწყობილობებისა და საბაზო სადგურებისთვის. სხვადასხვა ენერგეტიკულ პირობებში უსაფრთხოების სქემების სირთულე ადაპტიურად უნდა იყოს მორგებული. სხვადასხვა თავდასხმისადმი დაუცველობამ შეიძლება გავლენა მოახდინოს უსაფრთხოების სქემის ოპტიმიზაციაზე თავდასხმის მახასიათებლების ჰეტეროგენულობის გამო. კომპრომეტირებული პერიფერიული კვანძის ამოცნობა მოითხოვს უფრო დახვეწილ, AI-ზე დაფუძნებულ სქემებს, ვიდრე DDoS თავდასხმის გამოვლენა. გარდა ამისა, AI ტექნოლოგიები საშუალებას აძლევს არა მხოლოდ 6G ქსელებს, არამედ თავდამსხმელებს, განვითარდნენ წინა მავნე აქტივობების შესწავლით. უსაფრთხოების სქემები მუდმივად უნდა გაუმჯობესდეს განვითარებადი თავდამსხმელებისგან თავდასაცავად, უსაფრთხოების დონესა და ენერგიის მოხმარებას შორის კომპრომისის შეცვლით.

შემოთავაზებული სტრუქტურის დეტალურად საილუსტრაციოდ, წარმოვადგენთ სმარტფონისა და საბაზო სადგურის ორ შემთხვევას. ნახ. 4.2ა-ზე სმარტფონი აგროვებს ატრიბუტებს უსაფრთხოებასთან დაკავშირებული საფრთხეებიდან, ენერგეტიკული მდგომარეობიდან, მოწყობილობის სტატუსიდან, სერვისის ფუნქციებიდან და ასევე, ინფორმაციას მეზობელი რეგიონების საბაზო სადგურებიდან. ატრიბუტები გადაეცემა შემოთავაზებულ ოპტიმიზაციის სტრუქტურას და შეირჩევა ატრიბუტების ურთიერთ-

ქმედების მახასიათებლების საფუძველზე, რათა შემცირდეს მოდელის ტრენინგის სირთულე. გადაწყვეტა შეირჩევა ხელმისაწვდომი უსაფრთხოების სქემებიდან და კონფიგურირებულია სმარტფონისთვის უსაფრთხოებასა და ენერგეტიკას შორის ოპტიმალური კომპრომისის მისაღწევად. მაგალითად, როდესაც სმარტფონს აქვს მაღალი ენერგოტევადობა, მონაცემთა დაშიფვრისთვის კრიპტოგრაფიული გასაღების სიგრძე შეიძლება იყოს დიდი (მაგალითად, 1024 ბიტი), დაშიფვრის მაღალი საიმედოობისთვის. როდესაც ენერგიის მოხმარება დაბალია, გასაღების სიგრძე შეიძლება შემცირდეს (მაგალითად, 512 ბიტამდე), როგორც კომპრომისი, რათა შემცირდეს გამოთვლითი ოვერჰედი და გაიზარდოს მუშაობის დრო. ნახ. 4.2ბ-ზე, მოქმედება გადადის საბაზო სადგურზე, რომელსაც აქვს უფრო ადეკვატური ელექტრომომარაგება და უფრო მაღალი უსაფრთხოების პრიორიტეტი, ვიდრე სმარტფონს და მას შეუძლია აირჩიოს უფრო დახვეწილი სქემა და რთული კონფიგურაცია. საბაზო სადგურებზე უსაფრთხოების სქემები ოპტიმიზებულია ატრიბუტების სხვადასხვა ნაკრებით, მათ შორის: სერვისებით, თავდასხმის დაუცველობით, ტექნიკური შესაძლებლობებით, მომხმარებლის მოთხოვნებით, ქსელური გარემოთი და სხვა დროში ცვალებადი ატრიბუტებით. ვინაიდან საბაზო სადგურები იყენებენ განახლებად ენერგიას, როგორც ენერგიის ნაწილობრივ წყაროს, განახლებადი ენერგიის მიწოდების ცვალებადობა ასევე გამოიყენება, როგორც ენერგეტიკული სტატუსის მნიშვნელოვანი მაჩვენებელი. გარდა ამისა, დამატებითმა ატრიბუტებმა, როგორიცაა მეზობელი კვანძებიდან თავდასხმის გაფრთხილებები, ქსელური კომუნიკაციის მეტრიკა და დაკავშირებული მოწყობილობების სტატუსი, ასევე შეიძლება გავლენა იქონიოს უსაფრთხოებასა და ენერგეტიკას შორის კომპრომისზე. ამ შემთხვევაში, საბაზო სადგურის ატრიბუტების ნაკრები უფრო მრავალგანზომილებიანია, ვიდრე მომხმარებლის მოწყობილობების. ატრიბუტების დიდ რაოდენობასთან ურთიერთქმედების დახასიათების გასაადვილებლად, ფუნქციის აპროქსიმაცია ინტეგრირებულია შემოთავაზებულ მოდელირების მიდგომასთან. უსაფრთხოების სქემების ოპტიმალური გადაწყვეტის ფორმულირებით, როგორც ატრიბუტების ფუნქცია, ჩვენ მოვახდენთ კომპლექსურ აპროქსიმაციას ფურიეს უფრო მარტივი საბაზისო ფუნქციების სერიის მეშვეობით. აპროქსიმაციისთვის განკუთვნილი საბაზისო ფუნქციების რაოდენობის მინიმიზაციის გზით, დარჩენილ საბაზისო ფუნქციებში ჩართული ატრიბუტები შეიძლება შეირჩეს პირველი რაუნდისთვის. ამის შემდეგ, მოდელირების მიდგომა ამუშავებს შემცირებული განზომილების ატრიბუტებს ურთიერთქმედების მახასიათებლებით, რათა შეარჩიოს ატრიბუტები მეორე რაუნდისთვის. ოპტიმიზაციის მოდელი განახლდება იტერაციულად, რათა რეალურ დროში უზრუნველყოს ოპტიმალური უსაფრთხოების სქემის გადაწყვეტა საბაზო სადგურისთვის.

4.4.3. კომპიუტერული სიმულაციის შედეგები

ჩატარდა ვრცელი კომპიუტერული სიმულაციები უსაფრთხოების სქემის ოპტიმიზაციის კუთხით, რათა დადასტურებულიყო შემოთავაზებული სტრუქტურის ეფექტიანობა უსაფრთხოებისა და ენერგიის მოხმარების კომპრომისის დასაბალანსებლად, შესაბამისად, სმარტფონისა და საბაზო სადგურის სცენარებში. ორივე სცენარში უსაფრთხოების დონე და ენერგიის მოხმარება შედარებულია შემოთავაზებული ოპტიმიზაციის სტრუქტურის გამოყენებით და მის გარეშე, სხვადასხვა სერვისისა და ენერგიის მოხმარების პირობებში. გამოყენებული სერვისები მოიცავს ონლაინბანკინგს და ვიდეოსტრიმინგს, რაც წარმოადგენს უსაფრთხოების დონესთან დაკავშირებულ განსხვავებულ მოთხოვნებს. ბატარეის პირობებში შედის მაღალი და დაბალი ენერგოტევადობის შემთხვევები. კრიპტოგრაფიაზე დაფუძნებული სქემა და AI-ზე ორიენტირებული სქემა შეფასებულია სიმულაციების მიხედვით. ჩვენ ვიყენებთ გასაღების ზომას, რომელიც უნდა ასახავდეს კრიპტოგრაფიაზე დაფუძნებული სქემების საიმედოობასა და გამოვლენის სიხშირეს, რათა შევაფასოთ AI-ზე ორიენტირებული სქემების მახასიათებლები. ენერგიის

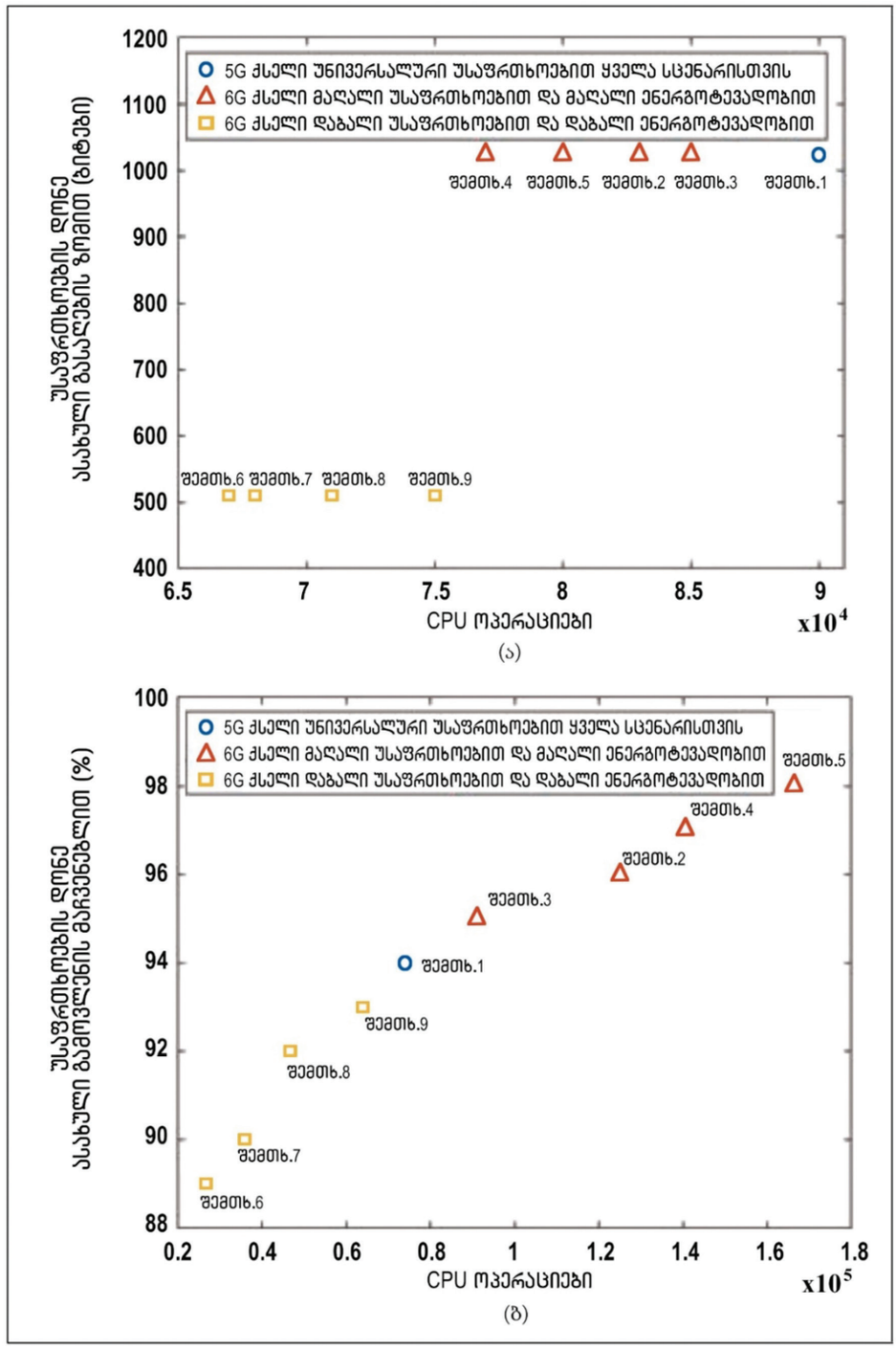
მოხმარება შეფასებულია CPU ოპერაციების რაოდენობის მიხედვით, რომელიც საჭიროა უსაფრთხოების სქემისთვის. ნახ. 4.5ა-ზე, კრიპტოგრაფიაზე დაფუძნებული სქემის ენერგიის მოხმარება, ასევე უსაფრთხოების დონე წარმოდგენილია კოორდინატებად და შეიძლება დაჯგუფდეს პირველ, მე-2 და მე-3 ჯგუფად, რომლებიც ნაჩვენებია შესაბამისად – წრეებით, სამკუთხედებითა და კვადრატებით. მე-2 ჯგუფი წარმოადგენს შემთხვევებს უსაფრთხოების მაღალი მოთხოვნებით და მაღალი ენერგოტევადობით 6G ქსელში. მე-2 ჯგუფის შესაბამისი სქემები იყენებენ უფრო გრძელ გასაღებებს და მოიხმარენ უფრო მეტ CPU ოპერაციებს, ვიდრე მე-3 ჯგუფის, რადგან მე-3 ჯგუფს აქვს დაბალი უსაფრთხოების მოთხოვნები და დაბალი ენერგომოხმარება. შედარებისთვის, პირველი ჯგუფი წარმოადგენს 5G უსაფრთხოებას და არ აქვს სხვა წერტილები სხვადასხვა შემთხვევისთვის მისი უნივერსალური კონფიგურაციის გამო. ვინაიდან ჩვენ ვიყენებთ გასაღების ზომას, როგორც უსაფრთხოების დონის მეტრიკას კრიპტოგრაფიაზე დაფუძნებული სქემებისთვის, სიმულაციის შედეგებში არჩეული გასაღების ზომებია 1024 ბიტი და 512 ბიტი. ამ მიზნით, 5G უსაფრთხოების სქემას აქვს ენერგიის ყველაზე მაღალი მოხმარება ყველა შემთხვევაში, მიუხედავად იმისა, რომ უსაფრთხოების მოთხოვნები და ენერგოტევადობა დაბალია. ანალოგიურად, როგორც ნაჩვენებია ნახ. 4.5ბ-ზე, უსაფრთხოების სქემის მეტრიკის კოორდინატები სხვადასხვა შემთხვევაში ასევე შეიძლება დაიყოს იმავე სამ ჯგუფად, როგორც ნახ. 4.5ა-ზე. ვინაიდან გამოვლენის სიხშირე გამოიყენება, როგორც უსაფრთხოების დონის მეტრიკა AI-ზე ორიენტირებული სქემებისთვის, უსაფრთხოების დონის ზრდა უფრო აშკარაა ნახ. 4.5ბ-ზე, ვიდრე ნახ. 4.5ა-ზე. უფრო მეტი CPU ოპერაციები იწვევს უსაფრთხოების უკეთეს დონეს, რომელიც შეიძლება მორგებული იყოს 6G უსაფრთხოების სქემებისთვის უსაფრთხოების სხვადასხვა მოთხოვნისა და ენერგიის მოხმარების შესაბამისად. 5G უსაფრთხოების ჯგუფი შუაშია მხოლოდ ერთი მნიშვნელობით, რადგან ის იყენებს მხოლოდ ერთ უნივერსალურ კონფიგურაციას. სიმულაციის შედეგები ადასტურებს, რომ როგორც სმარტფონებისთვის, ასევე საბაზო სადგურებისთვის, ისევე როგორც უსაფრთხოების სქემების ორივე კატეგორიისთვის, შემოთავაზებულ სტრუქტურას შეუძლია შეცვალოს 6G ქსელის უსაფრთხოება, რათა დააბალანსოს კომპრომისი უსაფრთხოებასა და ენერგეტიკას შორის. 5G-ის უსაფრთხოებასთან შედარებით, რომელიც იყენებს უნივერსალურ კონფიგურაციას ყველა სცენარისთვის, 6G-ის უსაფრთხოება ადაპტირებულია სხვადასხვა სერვისსა და ენერგეტიკულ პირობებზე. აქედან გამომდინარე, შემოთავაზებულ სტრუქტურას შეუძლია მნიშვნელოვნად გააუმჯობესოს უსაფრთხოება 6G ქსელში ენერგოეფექტიანობის თვალსაზრისით.

4.5. 6G-ის უსაფრთხოების ღია საკითხები

ვინაიდან 6G ქსელის შემუშავება ჯერ კიდევ საწყის ეტაპზეა, ბევრი ღია საკითხი რჩება მოსაგვარებელი 6G-ის უსაფრთხოების სამომავლო კვლევებში:

- პირველი, პერსპექტიული მიმართულებაა უსაფრთხოების სტრატეგიის ოპტიმიზაცია ქსელის ჰოლისტიკური სიტუაციის გაცნობიერებით. შემოთავაზებულ სტრუქტურაში, უსაფრთხოება კონფიგურირებულია მოწყობილობებიდან და მეზობელი პერიფერიული კვანძებიდან შეგროვებული ოპერატიული მონაცემების საფუძველზე. მომავალში, სიტუაციის ინფორმირებულობა შეიძლება გავრცელდეს ჰოლისტიკურ ქსელში, რათა უსაფრთხოებასთან დაკავშირებული ინფორმაცია იყოს გაზიარებული მოწყობილობებსა და საბაზო სადგურებს შორის ქსელის ინფრასტრუქტურის მასშტაბით, რათა მოხდეს თავდასხმების პროგნოზირება, ანალიზი და რეაგირება რეალურ დროში და, გარდა ამისა, თანამშრომლობით. საჭიროა შეიქმნას გლობალური პლატფორმა ინფორმაციის გაზიარებისთვის სხვადასხვა მოწყობილობასა და პერიფერიულ კვანძებს შორის. მომავალში წარმოიქმნება დამატებითი გამოწვევები: რა ინფორმაცია უნდა იყოს გაზია-

რებული და გაანალიზებული, რათა შემცირდეს გადაცემის ოვერჰედი და სწავლების სირთულე, როგორ დავიცვათ მომხმარებლის კონფიდენციალურობა ინფორმაციის გაზიარების დროს.



ნახ. 4.5. უსაფრთხოებასა და ენერგეტიკას შორის კომპრომისის ბალანსირების სიმულაციური შედეგები სხვადასხვა სცენარში, 5G და 6G ქსელებში განსხვავებული ინტელექტუალური სერვისებისა და ენერგეტიკული გამტარუნარიანობისთვის: ა) კრიპტოგრაფიაზე დაფუძნებული სქემისთვის; ბ) AI-ზე ორიენტირებული სქემისთვის. 9 შემთხვევა წარმოადგენს: (1) 5G ქსელს; (2) სმარტფონს ონლაინბანკინგისთვის; (3) სმარტფონს ბატარეის მაღალი ტევადობით; (4) საბაზო სადგურს ონლაინბანკინგისთვის; (5) საბაზო სადგურს ბატარეის მაღალი სიმძლავრით; (6) სმარტფონს ვიდეოსტრიმინგისთვის; (7) სმარტფონს ბატარეის დაბალი ტევადობით; (8) საბაზო სადგურს ვიდეოსტრიმინგისთვის; (9) საბაზო სადგურს ბატარეის დაბალი სიმძლავრით

- მეორე, 6G ქსელში თავდასხმის დაუცველობა რაოდენობრივად უნდა იყოს გაზომილი, რათა უსაფრთხოების დონის მოთხოვნები უფრო ზუსტად განისაზღვროს უსაფრთხოების სტრატეგიის ოპტიმიზაციისთვის. ასევე გასათვალისწინებელია თავდასხმების ევოლუცია და ცვალებადობა, რადგან AI-ის შეუძლია თავდამსხმელებს მისცეს შესაძლებლობა, ისწავლონ წინა ქმედებებიდან, რათა გვერდი აუარონ უსაფრთხოების მიმდინარე გადაწყვეტილებებს. ცრუ მონაცემების ინექციით გამოწვეული თავდასხმებისგან დაუცველობის შეფასება შესწავლილია 6G-ზე დაფუძნებულ ჭკვიან ქსელში, ღრმა სწავლების ტექნიკის საფუძველზე. მომავალში, მეტი კვლევითი ძალისხმევაა საჭირო, რათა შეიქმნას დაუცველობის გაზომვის უნივერსალური სტანდარტი სხვადასხვა მოწყობილობაზე, პერიფერიულ კვანძებსა და სერვისებზე სხვადასხვა თავდასხმისთვის.
- დაბოლოს, უსაფრთხოების სქემებსა და ენერგიის მოხმარებას შორის კავშირი საჭიროებს შემდგომ გამოკვლევას. ამჟამად, უსაფრთხოების სქემების ენერგიის მოხმარება ფასდება CPU-ის გამოყენების შესახებ ინფორმაციის მეშვეობით. მომავალში, შეფასება უნდა გაფართოვდეს სისტემურიდან ფიზიკურ დონემდე, რათა ენერგეტიკული სტატუსი შეგროვდეს უშუალოდ აპარატურიდან. ენერგოტევადობის ფაქტობრივი ცვლილებების მონიტორინგით, ჩვენ შეგვიძლია დავასკვნათ უსაფრთხოების სქემების მიერ შესრულებული შესაბამისი ოპერაციები, როგორიცაა ჰომომორფული დაშიფვრა და უსაფრთხო მრავალმხრივი გამოთვლა. თუ უფრო ზუსტი და პირდაპირი კავშირი დამყარდება უსაფრთხოებასა და ენერგეტიკას შორის, ჩვენ შეიძლება მივაღწიოთ უფრო ღრმა ხედვას 6G-ის უსაფრთხოების შესახებ, გამომდინარე ენერგოეფექტიანობის პერსპექტივიდან.

4.6. მეოთხე თავის დასკვნა

ამ თავში ჩვენ შევისწავლეთ ადაპტიური და დინამიკური უსაფრთხოება 6G ქსელში ენერგოეფექტიანობის თვალსაზრისით. გამოვიკვლიეთ AI-ზე დაფუძნებული 6G არქიტექტურა პერსპექტიული აპლიკაციებითა და ხედვებით. შემდეგ განვიხილეთ უსაფრთხოების საფრთხეები 6G-სთვის და უსაფრთხოების სტრატეგიის ოპტიმიზაციის გამოწვევები, გამომდინარე ჰეტეროგენულობის, დინამიკის და მოდელირების სირთულის ასპექტებიდან. გარდა ამისა, ჩვენ განვიხილეთ ოპტიმიზაციის სტრუქტურა გამოვლენილი პრობლემების გადასაჭრელად. შემოთავაზებული სტრუქტურა ოპტიმიზაციას უკეთებს უსაფრთხოების სქემის შერჩევას და კონფიგურაციებს, რათა დააბალანსოს კომპრომისი უსაფრთხოებასა და ენერგეტიკას შორის სხვადასხვა სცენარში. დაბოლოს, განვიხილეთ 6G-ის უსაფრთხოებასთან დაკავშირებული ღია საკითხები.

თავი 5. უსაფრთხოების ფუნქციის ვირტუალიზაცია საგნების ინტერნეტის მოწყობილობებისთვის 6G ქსელებში

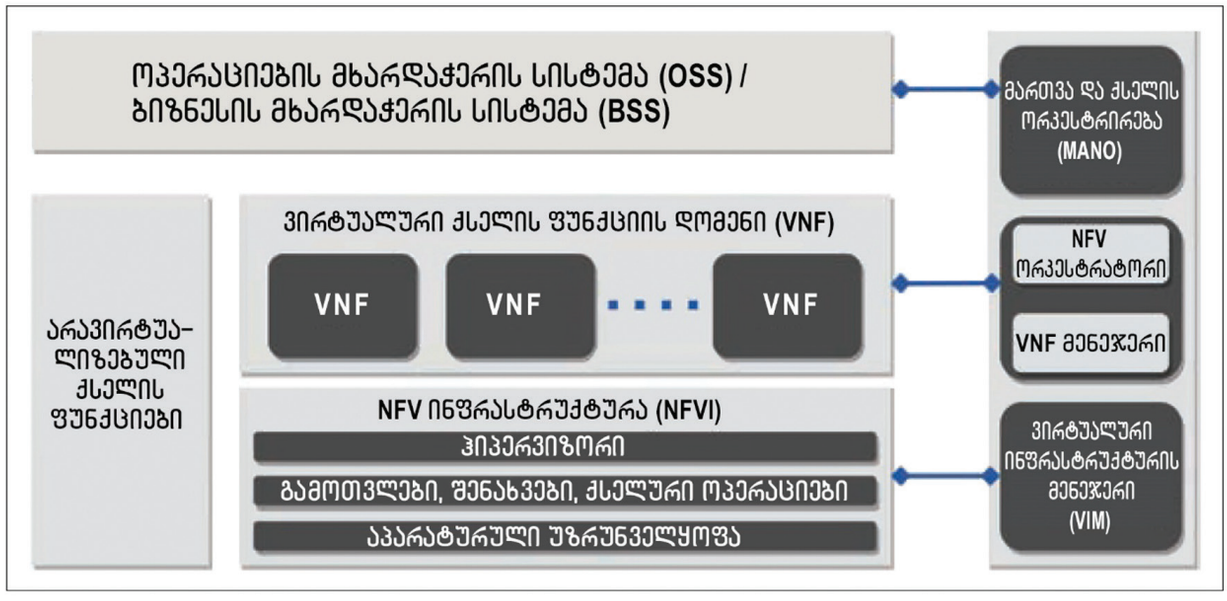
5.1. შესავალი

IoT მოწყობილობებს შეუძლიათ შეაგროვონ და გადასცენ მონაცემები ადამიანის ჩარევით და მის გარეშე. მოსალოდნელია, რომ IoT ითამაშებს კრიტიკულ როლს ავტომატიზაციის სტრატეგიებში, რათა შეასრულოს სხვადასხვა ამოცანა ადგილობრივად, დინამიკური კონტროლის სტრატეგიებით, მომავალი საინფორმაციო ქსელებისთვის, სადაც IoT მოწყობილობების ფუნდამენტური უპირატესობა მდგომარეობს მათ უნარში, დაუკავშირდნენ შედარებით მოკრძალებული ტექნიკის სპეციფიკაციებს. 6G განიხილება, როგორც გადასვლა დაკავშირებული საგნებიდან დაკავშირებულ ინტელექტზე. ეს ნიშნავს, რომ IoT მოწყობილობებს მოუწევთ დიდი რაოდენობით ინფორმაციის გაზიარება ერთმანეთთან, რაც გამოიწვევს უსაფრთხოების სხვადასხვა პრობლემას. იმის გამო, რომ 6G IoT იყენებს მაღალი სიმკვრივის ინტერნეტით დაკავშირებულ ჰეტეროგენულ მოწყობილობებს (მაგალითად, სენსორებს, სმარტფონებს, დახურულ სატელევიზიო (CCTV) კამერებს, აქტივატორებს), რომლებიც მხარს უჭერენ უფრო მძლავრი სისტემის არქიტექტურას, საჭიროებენ მაღალ ტევადობას და AI-ზე დაფუძნებულ ჭკვიან ალგორითმებს, უსაფრთხოების პრობლემები კიდევ უფრო მეტად თვალსაჩინო და დამძიმებულია, რაც IoT-ს კიდევ უფრო დაუცველს ხდის კიბერთავდასხმების მიმართ. მათ შორის, მავნე პროგრამები მზარდი შეშფოთების საგანია და ამიტომ, სანდოობა გადამწყვეტია IoT სისტემებისთვის 6G ქსელებში.

ინფრასტრუქტურული ლინკები ან D2D კომუნიკაციის ლინკები შეიძლება გამოყენებულ იქნეს IoT სისტემებში მავნე პროგრამების გასავრცელებლად. მისამართების სივრცის სკანირება, Telnet და პაროლის უხეში ძალით გატეხვა, შეიძლება გამოყენებულ იქნეს IoT მოწყობილობების კომპრომეტირებისთვის ინფრასტრუქტურული ლინკების გამოყენებით. D2D ლინკების საშუალებით მავნე პროგრამების გავრცელების მაგალითებია Cabir და Commwarror მობილური ჭიები, რომლებიც იყენებდნენ Bluetooth-ის Symbian-ზე დაფუძნებულ მობილურ ტელეფონებს შორის გასავრცელებლად. IoT მოწყობილობებმა შეიძლება გამოიყენონ სხვადასხვა უსადენო სტანდარტი (როგორიცა Zigbee) ერთმანეთთან კომუნიკაციისთვის. ამრიგად, მკვლევრებმა აჩვენეს მავნე პროგრამების გავრცელების შესაძლებლობა სიახლოვეზე დაფუძნებული (proximity-based) უსადენო ინტერფეისებით. იმისდა მიუხედავად, თუ როგორ ვრცელდება მავნე პროგრამა, დაუცველი და დაუმუშავებელი IoT მოწყობილობები ზრდის მავნე პროგრამის თვითგამრავლების რისკს. მიუხედავად იმისა, რომ ზოგიერთ IoT მოწყობილობას შეიძლება ჰქონდეს უსაფრთხოების პატჩები, მათი ინსტალაცია რჩება უკიდურესად ძვირად ღირებული და პრაქტიკაში ეფექტური არ არის. ეს აშკარად ჩანს ბოლოდროინდელი კვლევებიდან, რომელიც აჩვენებს, რომ IoT მოწყობილობებში დაუცველობის 95 პროცენტი დაკავშირებულია firmware-სთან (firmware არის SW, რომელიც წარმოგვიდგენს ძირითად მანქანურ ინსტრუქციებს, რომლებიც საშუალებას აძლევს HW-ის ფუნქციონირდეს და დაუკავშირდეს მოწყობილობაზე გაშვებულ სხვა SW-ს). IoT მოწყობილობის firmware შეიძლება იყოს გატეხილი ან თუნდაც, გამოყენებულ იქნეს მავნე პროგრამების გასავრცელებლად ქსელის სხვა სუბიექტებზე. გარდა ამისა, კონკრეტული მოწყობილობების შესახებ ლიტერატურაში მოხსენიებული დაუცველობა ასევე ექვემდებარება ჰაკერულ თავდასხმებს. თუმცა, ამ მოწყობილობების აქტიური მოვლის არარსებობის და ხანგრძლივი სიცოცხლის გამო, ისინი, როგორც წესი, არ არიან იმუნური ასეთი დაუცველობისგან. ინფორმირებულობის ნაკლებობა და გა-

დაჭარბებული შეფერხება, რომელიც დაკავშირებულია უსაფრთხოების განახლებების ან პატჩების ინსტალაციასთან, იწვევს იმას, რომ ბევრი IoT მოწყობილობა არ იღებს დროულად firmware განახლებებს ან უსაფრთხოების პატჩებს. ეს მავნე პროგრამას საშუალებას აძლევს, გავრცელდეს IoT ქსელებში იდენტიფიკაციის გარეშე.

ჩაშენებულ მოწყობილობებზე გაშვებული SW-ის მთლიანობის შემოწმებისა და მავნე პროგრამის აღმოჩენის პროცესს ატესტაცია ეწოდება. ატესტაციის არსებული ტექნიკა ან გამოთვლითი კუთხით ძალიან რთულია IoT მოწყობილობებისთვის ან ეყრდნობა სპეციალიზებულ არქიტექტურებს. ამრიგად, შეუძლებელია ჰეტეროგენული მოწყობილობების ფართო სპექტრის უზრუნველყოფა HW-ზე დაფუძნებული გადაწყვეტილებებით. 5G-ის ერთ-ერთი მთავარი თვისება არის NFV, რომელიც სისტემას საშუალებას აძლევს, გაანაწილოს თავისი რესურსები და სერვისები ვირტუალიზაციის გამოყენებით, ქსელის კვანძების ფუნქციების მთელი კლასის ვირტუალიზაციისთვის სამშენებლო ბლოკებში, რომლებიც შეიძლება ერთმანეთს დაუკავშირდნენ ან შექმნან ჯაჭვები სხვადასხვა საკომუნიკაციო სერვისის განსახორციელებლად, როგორც ნაჩვენებია ნახ. 5.1-ზე.



ნახ. 5.1. NFV არქიტექტურის წარმოდგენა მისი ინტერფეისებით

ქსელის ფუნქციების SW-ის ზოგიერთი უპირატესობა მოიცავს ქსელის ოპერაციების გამარტივებას, ექსპლუატაციის ხარჯების შემცირებას, რესურსების უკეთ გამოყენებასა და ქსელის აპარატურული ციკლების გახანგრძლივებას გამოყოფილი ტექნიკისა და აღჭურვილობის საჭიროების აღმოფხვრის გზით. ეს იწვევს უფრო მაღალ მასშტაბურობას ქსელში დაკავშირებული მოწყობილობების შედარებით მეტი რაოდენობის მხარდასაჭერად. თუმცა, 6G-ით, მასშტაბურობა კიდევ უფრო უნდა გაფართოვდეს. ამიტომ, ამ პრობლემის გადასაჭრელად, ეს თავი გვთავაზობს უსაფრთხოების სტრუქტურას, რომელიც დაფუძნებულია უსაფრთხოების ფუნქციის SW-ზე, რათა ჩართოს ვირტუალური დისტანციური ატესტაცია; ანუ ქსელის ფუნქციების ვირტუალიზაციის გარდა, ჩვენ განვიხილავთ უსაფრთხოების ფუნქციის ვირტუალიზაციასაც. გასათვალისწინებელია, რომ SFV, ეს არის NFV-ის ახალი განშტოება 6G ქსელებში, რომელიც იყენებს იგივე NFV პრინციპებს უსაფრთხოების სერვისების მასშტაბური შეთავაზებისთვის.

ყოვლისმომცველი კომუნიკაციის ბოლოდროინდელი მიღწევებიდან გამომდინარე, 6G ქსელებში გავრცელებული მავნე პროგრამა წარმოადგენს უსაფრთხოების პრობლემას, რომელიც საგანგაშო ტემპით

იზრდება. ეს თავი განიხილავს ამ საკითხს უსაფრთხოების სტრუქტურის შემოთავაზებით, რომელიც იყენებს NFV-ს SFV-სთან ერთად SW-ის ინსტალაციისთვის ქსელის მდებარეობებზე და მავნე პროგრამის გავრცელებას ეფექტიანად აკავებს. ის ასევე გამორიცხავს HW-ის ნებისმიერი ინფრასტრუქტურის საჭიროებას შემდეგი თვისებების შეთავაზებით:

მასშტაბურობა: არსებობს მუდმივი საჭიროება უფრო მოქნილი მიდგომის მიმართ, სერვისის მიწოდების კუთხით შემდეგი თაობის საკომუნიკაციო ქსელებში, რადგან მომხმარებლის მოთხოვნებს აქვს სწრაფად ცვალებადი დინამიკური ლანდშაფტი. აქედან გამომდინარე, საკომუნიკაციო ინფრასტრუქტურას უნდა ჰქონდეს მოქნილობა, რათა ქსელის ოპერატორებს შეეძლოთ ადვილად გააფართოონ თავიანთი ქსელები სერვერებს შორის.

უსაფრთხოება: პირდაპირი სერვისის პროვაიდერები ჩვეულებრივ ზრუნავენ უსაფრთხოებაზე, რომლის მიღწევაც სურთ და ამით მიისწრაფვიან უფრო მეტი კონტროლისკენ, მათი ქსელის მართვის პროცესში. SFV საბოლოო მომხმარებლებს ანიჭებს შესაძლებლობას, ამ ქსელებში გამოიყენონ ვირტუალური მანქანა, არსებული firewall-ების გვერდით.

მოქნილობა: სატელეკომუნიკაციო ოპერატორებისთვის წინა პირობაა ახალი სერვისების უწყვეტი გამოყენება. ამრიგად, სამომავლო საინფორმაციო ქსელები უნდა იყოს შედარებით ადაპტირებადი, მარტივი ინსტალაციისა და უზრუნველყოფის უპირატესობებით, ქსელებში სხვადასხვა ფუნქციის უწყვეტი ინტეგრაციით.

ღირებულება: ქსელის ოპერატორებმა და სერვისის პროვაიდერებმა უნდა უზრუნველყონ ოპტიმალური ფასები მომხმარებლის შესანარჩუნებლად და ასევე, მათი სამომხმარებლო ბაზის გაზრდისთვის. ამის მისაღწევად, მონაცემთა ცენტრები უნდა განლაგდეს უკვე არსებული ვენდორების მხარდაჭერით.

ჩატარებული კვლევების მოკლე მიმოხილვა წარმოდგენილია მომდევნო პარაგრაფში. ამის შემდეგ მოცემულია ქსელის მოდელის მიმოხილვა, რომელიც აღწერს IoT მოწყობილობების დინამიკას, დაფუძნებულს NFV-სა და SFV-ზე და ახსნილია უსაფრთხოების სტრუქტურა IoT ქსელებში მავნე პროგრამების შეკავებისთვის. შემოთავაზებული სტრუქტურის ეფექტიანობის დემონსტრირებისთვის განიხილება მახასიათებლების ანალიზი, რომელიც აჩვენებს, თუ როგორ შეიძლება, ამ სტრუქტურამ მნიშვნელოვნად შეაკავოს მავნე პროგრამის გავრცელება. დასასრულ კი ამ თავის შედეგებია შეჯამებული.

5.2. ჩატარებული კვლევების მოკლე მიმოხილვა

მავნე პროგრამების გავრცელება IoT ქსელებში შეიძლება აღწერილი იყოს ადამიანებში ეპიდემიების გავრცელების ანალოგიურად. ამრიგად, თანამედროვე ლიტერატურაში მავნე პროგრამების სქემები და სტრუქტურები აგებულია ინფექციის ჰომოგენური გზით გავრცელების საფუძველზე, ეპიდემიოლოგიური მოდელების იდეის გათვალისწინებით. იგულისხმება, რომ მავნე პროგრამები ამჟამად კარგად დამკვიდრებულ შემსუბუქების მოდელებში, როგორებიცაა: „მგძნობელობა-ინფიცირება-აღდგენა“ და „მგძნობელობა-გამოვლენა-ინფიცირება-აღდგენა“ ერთდროულად იქნება გამოვლენილი და გამოსწორებული ქსელის ყველა მოწყობილობაში ან კვანძში. ფაქტობრივად, ეს ასახავს მდგომარეობის გადასვლას „ინფიცირებულიდან“ „გამოჯანმრთელებულამდე“, თუმცა, როგორც წესი, შეუძლებელია კომპრომეტირებული IoT მოწყობილობის უშუალო შეკეთება უსაფრთხოების პატჩების მიუწვდომლობის გამო. აქედან გამომდინარე, ბევრად მიზანშეწონილია მისი დაფიქსირება ინფრასტრუქტურის მხარეს (ანუ მისი კომუნიკაციების შეზღუდვა). ეს იწვევს მავნე პროგრამების შემდგომი გავრცელების შეზღუდვას. ამრიგად, „მგძნობელობა-ინფიცირება-აღდგენა“ მოდელის პრინციპების გამოყენებით, IoT სისტემაში ინფრასტრუქტურული ლინკები შეიძლება ჩაითვალოს, როგორც „აღდგენილი/დიაგნოზირებული“,

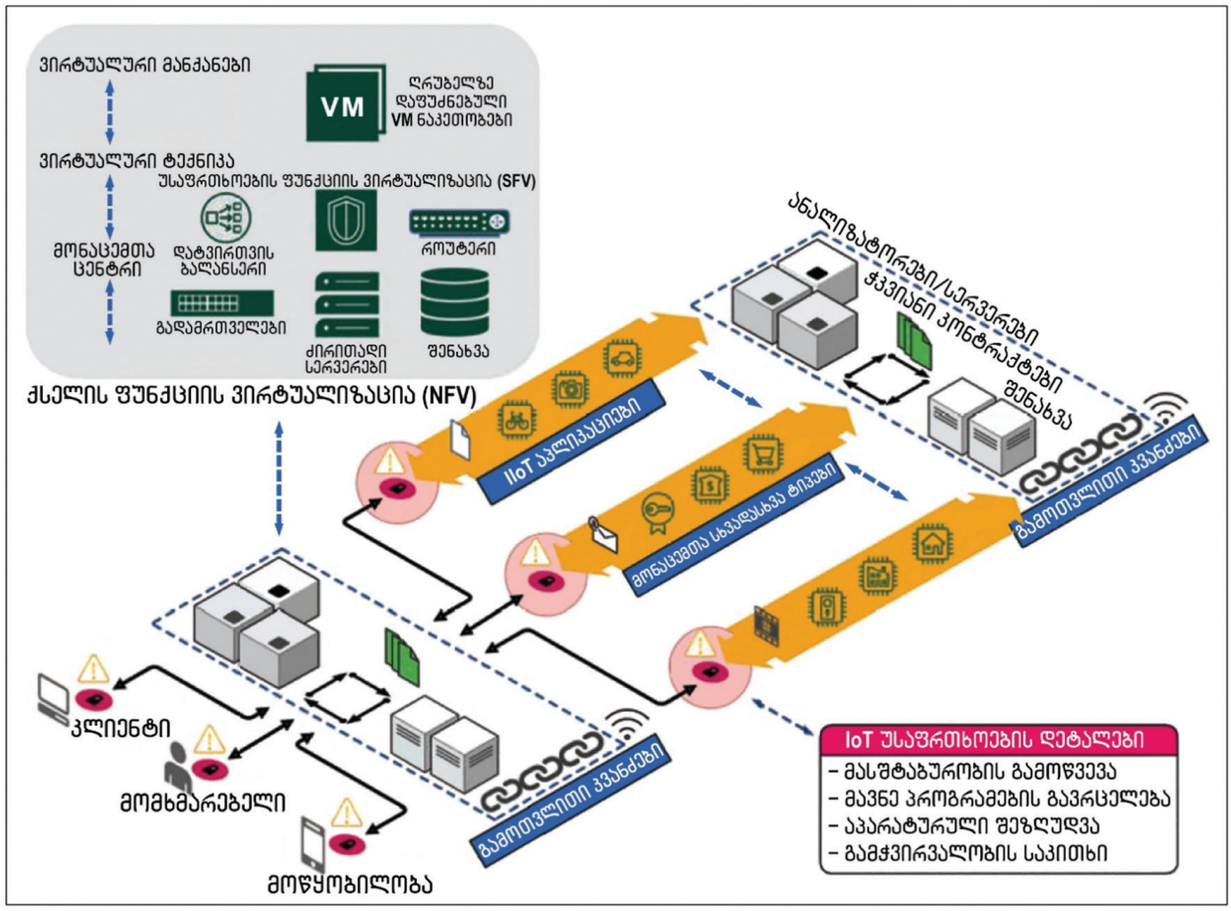
ხოლო კომპრომეტირებული მოწყობილობა რჩება „ინფიცირებული“. ეს არის ეფექტიანი გადაწყვეტა, რადგან ის ბლოკავს და იზოლირებს მავნე პროგრამას, რაც მის გავლენას ზღუდავს. თუმცა, ის ავლენს შუალედურ კვანძებს სხვადასხვა თავდასხმაზე (როგორიცაა ფიზიკური თავდასხმები). ასევე იწვევს დამატებით დამოკიდებულებას შუალედურ კვანძებზე. უფრო მეტიც, დასკვნა, რომ მავნე პროგრამების შეზღუდვა IoT გარემოში შეიძლება ჩაითვალოს „ლინკის აღდგენის“ პრობლემად, ნაცვლად „კვანძის აღდგენისა“, მოტივაციას უქმნის IoT მავნე პროგრამების შემსუბუქების მოდელების დამუშავებისა და ფორმულირების კიდევ ერთ განვითარებას.

ლიტერატურაში განხილული იყო მობილური IoT ქსელების ტრაფიკის მხედველობაში მიღებით შემუშავებული პატჩის დადების სქემა. ტრადიციული მეთოდებისგან განსხვავებით, სადაც მოწყობილობა უშუალოდ არის პატჩით შესწორებული, შემოთავაზებულ იქნა მნიშვნელოვანი შუალედური კვანძების პატჩით შესწორება. მობილური IoT მოწყობილობების მიერ წარმოქმნილი ტრაფიკის მოცულობის გამოყენებით, ნაჩვენები იქნა, რომ ეს წარმატებით შეზღუდავს მავნე პროგრამის გავრცელებას პირდაპირ D2D კავშირზე, რითაც მავნე პროგრამის გავლენა შემცირდება. თუმცა, შუალედურ კვანძებზე დამოკიდებულება, რაც იწვევს პატჩის დადების უფრო მეტ დროს, ამ წინადადებას ნაკლებად მიმზიდველს ხდის. ასევე, შემოთავაზებული იყო ML-ზე დაფუძნებული ტექნიკა, IoT ქსელებში მავნე პროგრამების გამოსავლენად. მხარი დაუჭირეს ასეთი სქემის ინტეგრირებას მოწყობილობაში პატჩის გამოყენების მოდელთან, რამაც უზრუნველყო განაწილებული უსაფრთხოების არქიტექტურა ქსელის ფუნქციების ვირტუალიზაციის ტექნიკის გამოყენებით. მიუხედავად იმისა, რომ აღნიშნული სტრუქტურა მასშტაბირებადია ქსელის ზომის მიხედვით, ის არსებითად, შრომატევადია ფუნქციის ვირტუალიზაციის ტექნიკის გამო და დაუცველია ფიზიკური თავდასხმების მიმართ. ასევე, შემოთავაზებულ იქნა დამაინტრიგებელი ფორმულირება, რომელშიც იკვლევდნენ სოციალური ქსელების სტრუქტურას, რათა დადგინდეს, თუ როგორ აისახება ის ეპიდემიის დაავადების გავრცელების დინამიკაზე სპეციალური (ad hoc) ქსელების აპლიკაციებით. განიხილეს ეპიდემიის გავრცელების მოდელი, რომელიც დაფუძნებულია „მგძნობელობა-გამოვლენა-ინფიცირება-აღდგენა“ მოდელზე მოსახლეობის აგრეგაციის სხვადასხვა დონისთვის. შემდეგ გააანალიზეს და გამოიყენეს მოდელის დინამიკა მობილური ad hoc ქსელებისთვის (MANET), რათა უკეთ გაეგოთ ამ ქსელებში მავნე პროგრამების გავრცელების დინამიკა. გარდა ამისა, წარმოდგენილ იქნა კიდევ ერთი დამაინტრიგებელი პატჩის დადების მექანიზმი სისტემებში ავტომატური პატჩის დადების შესაფასებლად, ანალიტიკური სტრუქტურის გამოყენებით. ეს მექანიზმი საშუალებას იძლევა, დროულად გაიგზავნოს „მკაფიო განახლების“ შეტყობინება ინფიცირებულ მოწყობილობებზე. ამ დროულმა რეაგირებამ შეიძლება, თავიდან აიცილოს პატჩი/ვირუსის შეჯიბრის მდგომარეობა, რაც ხელს უწყობს მოწყობილობების პატჩით უკეთ შეკეთებას. მიუხედავად იმისა, რომ ასეთი განახლებები შეიძლება სასიცოცხლო მნიშვნელობის იყოს, განახლებების გაგზავნა ყოველ ჯერზე, როდესაც მოწყობილობა ინფიცირდება ან კომპრომეტირებულია, ზრდის დროით დანახარჯებს. აქედან გამომდინარე, საჭიროა პატჩის დადების „მსუბუქი“ მეთოდები, რომლებიც მოითხოვს დაბალ დროით დანახარჯებს მათი მუშაობისთვის.

ზემოთქმულიდან გამომდინარე, არსებული სტრუქტურების უმეტესობას აწუხებს ორი პრობლემა: პირველი, დროის ხანგრძლივი პერიოდი, ანუ მავნე პროგრამით ინფიცირებული მოწყობილობისთვის პატჩის დადებაზე დახარჯული დროის მაღალი ღირებულება; მეორე, მავნე პროგრამების გავრცელების შეზღუდული კონტროლი, ანუ კომპრომეტირებული მოწყობილობების იზოლაციის არარსებობა. ამ გამოწვევის საპასუხოდ, ეს თავი გვთავაზობს უსაფრთხოების იაფფასიან სტრუქტურას IoT გარემოსთვის, რომელსაც შეუძლია ეფექტიანად შეზღუდოს მავნე პროგრამების გავრცელება ქსელის იზოლაციის სამი კატეგორიის განსაზღვრის გზით და ქსელის ნაწილებად დაყოფის გამოყენებით.

5.3. ქსელის მოდელი და შემოთავაზებული სტრუქტურა

შემოთავაზებული უსაფრთხოების სტრუქტურის ქსელის მოდელი ნაჩვენებია ნახ. 5.2-ზე შემდეგი ძირითადი ბლოკებით.



ნახ.5.2. ბლოკჩეინზე დაფუძნებული ქსელის მოდელის მიმოხილვა SFV-ით და NFV-ით. განაწილებული გამოთვლითი კვანძები განათავსებენ ბლოკჩეინს და უზრუნველყოფენ საბოლოო მომხმარებლებს NFV სერვისებით, SFV-სთან ერთად

IoT მოწყობილობები: ეს წარმოადგენს საბოლოო მომხმარებლებს, რომელიც შეიძლება იყოს მოწყობილობა ან სენსორი. უნდა გავითვალისწინოთ, რომ თითოეული მოწყობილობა განიხილება, როგორც ჩაშენებული სისტემა ჩიპზე.

სერვერი: ეს არის სანდო სერვერი, რომელიც პასუხისმგებელია IoT მოწყობილობების რეგისტრაციაზე, მართვაზე, კონტროლსა და პატჩის დადებაზე.

ინფრასტრუქტურაზე დაფუძნებული ლინკები: IoT მოწყობილობები შეიძლება დაკავშირებული იყოს ინფრასტრუქტურაზე დაფუძნებულ საკომუნიკაციო ტექნოლოგიებთან, როგორიცაა ნებისმიერი თაობის მობილური სატელეკომუნიკაციო სისტემები, ფიჭური საბაზო სადგურების მეშვეობით და WiFi უსადენო ადგილობრივი ქსელის (WLAN) AP-ების მეშვეობით. თუმცა, IoT მოწყობილობების უმეტესობა არ ახდენს სრული TCP/IP სტეკის რეალიზაციას. ამიტომ, ისინი უნდა დაუკავშირდნენ ფიჭურ საბაზო სადგურებს და WLAN AP-ებს კარიბჭეების მეშვეობით, როგორიცაა IPv6 დაბალი სიმძლავრის უსადენო პერსონალურ ქსელებზე (6LoWPAN) დაფუძნებული როუტერის ელემენტები. ეს სასაზღვრო

როუტერის ელემენტები მოქმედებენ, როგორც კარიბჭეები, IoT მოწყობილობებისთვის ინტერნეტთან დასაკავშირებლად.

D2D ლინკები: IoT მოწყობილობებს შეუძლიათ დაუკავშირდნენ ერთმანეთს სიახლოვეზე დაფუძნებული უსადენო ინტერფეისებით, როგორიცაა პირდაპირი WiFi (WiFi Direct), დაბალი ენერგიის Bluetooth (BLE) და ახლო ველის კომუნიკაცია (NFC).

გამოთვლითი კვანძები: ეს წარმოადგენს მოწყობილობებს (განაწილებულ სერვერებს), რომლებიც ფუნქციონირებენ NFV-ზე და SFV-ზე დაფუძნებული ფუნქციების/სერვისების საბოლოო მომხმარებლებისთვის მიწოდების უზრუნველსაყოფად.

ამ პარაგრაფში განიხილება ახალი უსაფრთხოების სტრუქტურა და NFV-ის როლი 6G IoT სისტემებისთვის. შემოთავაზებული სტრუქტურის ბლოკ-სქემა ნაჩვენებია ნახ. 5.3-ზე. ამ ნახაზიდან ჩანს, რომ სანამ IoT მოწყობილობა დაიწყებს შემოთავაზებულ სტრუქტურასთან ურთიერთქმედებას, ის ჯერ უნდა დარეგისტრირდეს. მას შემდეგ, რაც დარეგისტრირდება, სტრუქტურა ამოწმებს, არის თუ არა იგი სანდო. იმისათვის, რომ მოწყობილობა იყოს სანდო, სტრუქტურა იყენებს SFV-ზე დაფუძნებულ დისტანციური ატესტაციის პროცედურას.

5.3.1. დისტანციური ატესტაცია

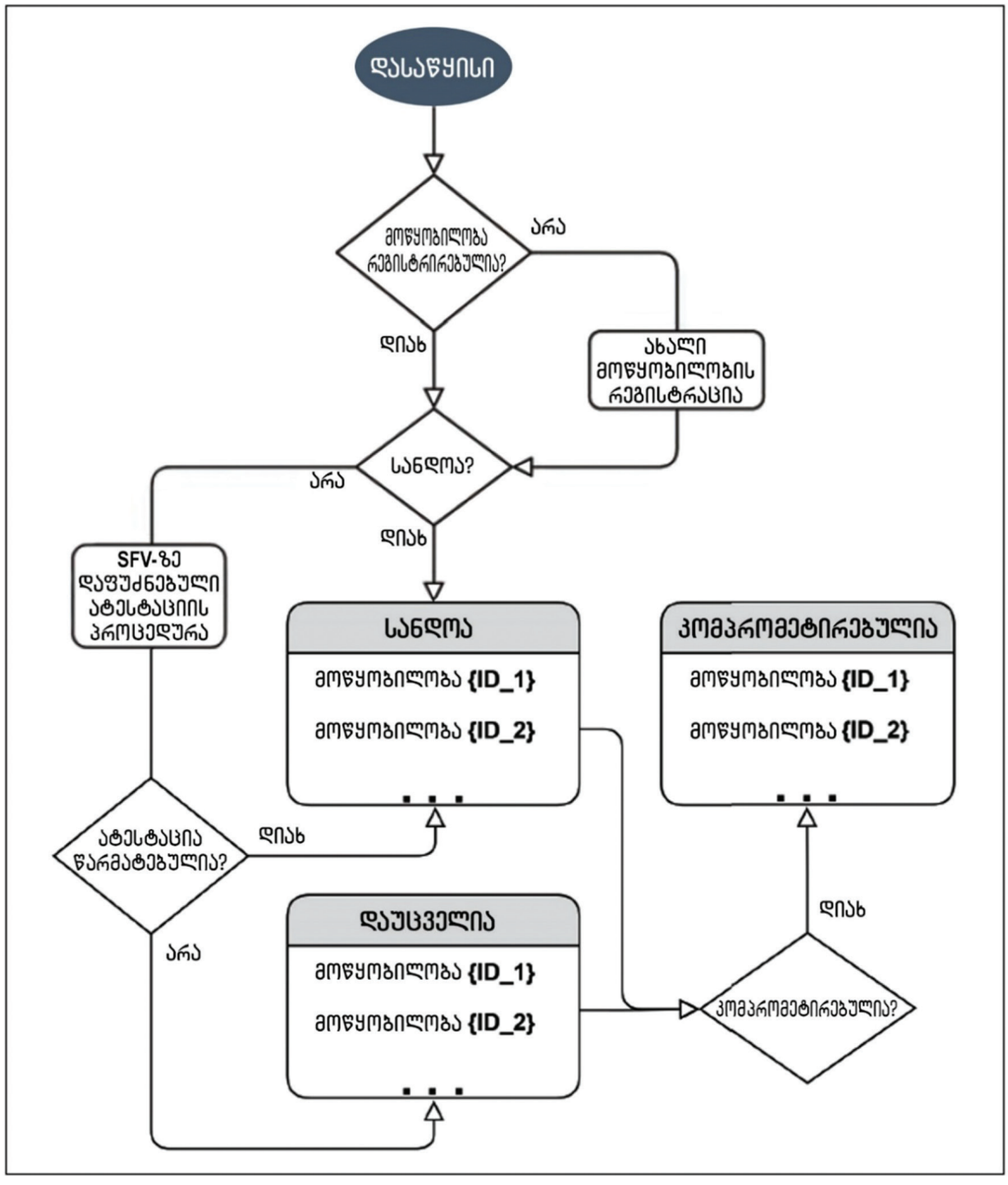
ატესტაცია არის ჩაშენებულ მოწყობილობაზე გაშვებული SW-ის უნებლიე და მავნე ცვლილებების გამოვლენის პროცესი მისი შიდა მდგომარეობის მთლიანობის უზრუნველსაყოფად. ალტერნატიულად, პროცესს, რომლის დროსაც სანდო სუბიექტი (ჩვეულებრივ მოხსენიებული, როგორც ვერიფიკატორი) იწყებს ატესტაციის პროცედურას დისტანციურად, ეწოდება დისტანციური ატესტაცია, ხოლო ჩაშენებული მოწყობილობა (ჩვეულებრივ, დამამტკიცებელს უწოდებენ) ამოწმებს მის შიდა მდგომარეობას. ატესტაციის პროცესის დასაწყებად, ვერიფიკატორი გამოწვევას უგზავნის დამამტკიცებელს. ამ გამოწვევის გამოყენებით, დამამტკიცებელი ითვლის მისი მეხსიერების შიგთავსის ჰეშ-დაიჯესტს და ვერიფიკატორთან აბრუნებს პასუხს, რომელსაც ეწოდება საკონტროლო ჯამი. შემდეგ, ვერიფიკატორი ამოწმებს საკონტროლო ჯამს, რათა დაადგინოს, დამამტკიცებელი კომპრომეტირებულია თუ არა.

ამ თავში ჩვენ ვიყენებთ ჰიბრიდული ატესტაციის (HAtt) პროცედურას, რომელიც არის ახლახან შემოთავაზებული, როგორც დისტანციური ატესტაციის ტექნიკა IoT მოწყობილობებისთვის. ჩვენ ავირჩიეთ ეს პროცედურა მისი უკიდურესად დაბალი დროითი და უსაფრთხოების ხარჯების გამო. კონკრეტულად, HAtt ყოფს IoT მოწყობილობის მეხსიერებას ბლოკებად და აღმოაჩენს ნებისმიერ მავნე ცვლილებას IoT მოწყობილობის SW-ში მეხსიერების ბიტების შემთხვევითი შერჩევის გზით. HAtt არის მარტივი პროცედურა, რომლის ვირტუალიზაცია შესაძლებელია SFV-ის საშუალებით, რათა იმუშაოს IoT მოწყობილობაზე მის ნორმალურ მუშაობაში ჩარევის გარეშე.

როგორც კი მოწყობილობა ატესტაციას წარმატებით გაივლის, ის ჩამოთვლილია სანდო მოწყობილობების კატეგორიაში. წინააღმდეგ შემთხვევაში, დაუცველთა კატეგორიაში აღმოჩნდება. დაუცველთა კატეგორიის მოწყობილობებმა უნდა გაიარონ ატესტაციის პროცედურა და მოიპოვონ სანდოობის სტატუსი. თუ რომელიმე კატეგორიაში ჩამოთვლილი მოწყობილობა კომპრომეტირებულია მავნე პროგრამით, სტრუქტურას ის გადააქვს კომპრომეტირებული მოწყობილობების კატეგორიაში. ამრიგად, მავნე პროგრამა ვერ გავრცელდება. ქსელის სამი კატეგორია შექმნილია ქვემოთ აღწერილი მიდგომების მიხედვით.

5.3.2. ქსელის იზოლაციის დონეები

შემოთავაზებულ სტრუქტურაში, ჩვენ ვიყენებთ NFV-ზე დაფუძნებულ ქსელის ნაწილებად დაყოფას, რათა ქსელის სამ განსხვავებულ იზოლაციის დონეზე დანაწევრება მოხდეს. გასათვალისწინებელია, რომ ეს დონეები განისაზღვრება IoT მოწყობილობების გამორჩეული ქცევით.



ნახ.5.3. შემოთავაზებული სტრუქტურის ბლოკ-სქემა

სანდო ნაწილი: IoT მოწყობილობები, რომლებიც არ არის კომპრომეტირებული და მავნე პროგრამებისგან თავისუფალია, ემატება ქსელის იზოლაციის სანდო დონეს. ამ კატეგორიაში, IoT მოწყობილობებს შეუძლიათ ერთმანეთთან კომუნიკაცია ნებისმიერი ხელმისაწვდომი საკომუნიკაციო ინტერფეისის საშუალებით.

დაუცველი ნაწილი: მკაცრი ქსელი გამოიყენება IoT მოწყობილობების დასამატებლად, რომლებიც ახალია მომხმარებლის ქსელში ან შეიძლება იყოს კომპრომეტირებული. ამ მოწყობილობების მიერ გენერირებული ტრაფიკი იფილტრება, რათა თავიდან იქნეს აცილებული მავნე პაკეტების ან კავშირის მოთხოვნების გაგზავნა გარე ქსელში, ან სხვა IoT მოწყობილობებზე.

კომპრომეტირებული ნაწილი: კომპრომეტირებული IoT მოწყობილობები ჩამოთვლილია იზოლირებულ დონეზე. გასათვალისწინებელია, რომ IoT მოწყობილობებმა შეიძლება გამოიყენონ სხვადასხვა საკომუნიკაციო ინტერფეისი, მათ შორის: Bluetooth, LTE და WiFi. ამ კატეგორიაში, IoT მოწყობილობები შემოიფარგლება ერთი ძირითადი საკომუნიკაციო ინტერფეისით, როგორიცაა WiFi. გარდა ამისა, ამ მოწყობილობებიდან გენერირებული ყველა შეტყობინება და კავშირის მოთხოვნა დაბლოკილია/გაუქმებულია.

აქვე უნდა აღინიშნოს, რომ შემოთავაზებული სტრუქტურის პროცედურის განმავლობაში, IoT მოწყობილობების მდგომარეობა მუდმივად იცვლება. მნიშვნელოვანია თვალყური ვადევნოთ ამ მდგომარეობების განახლებებს, რომლებიც დაგვეხმარება მავნე პროგრამების იდენტიფიცირებაში. შემოთავაზებული სტრუქტურა იყენებს ბლოკჩეინს, სამუშაოს მტკიცებულების კონსენსუსის შეცვლილ ვერსიას, ანუ მის დინამიკურ ვარიანტს ახალი ბლოკების მოსაპოვებლად. ეს ბლოკჩეინს საშუალებას აძლევს გააფართოოს სისტემა და დააკმაყოფილოს სისტემაში IoT მოწყობილობების მზარდი რაოდენობა.

5.3.3. სტრუქტურის მუშაობა

ნახ. 5.2 გვთავაზობს NFV-ის და მისი კომპონენტების მიმოხილვას ბლოკჩეინზე დაფუძნებული 6G ქსელისთვის. ამ ნახაზიდან ჩანს, რომ SFV მოქმედებს, როგორც ვირტუალური მოწყობილობა, რომელიც უზრუნველყოფს უსაფრთხოების სხვადასხვა მახასიათებელს, როგორიცაა მავნე პროგრამების გამოვლენა და აღმოფხვრა. სწორედ აქ მუშაობს შემოთავაზებული სტრუქტურა და ნახ. 5.3 აჩვენებს მის ფუნქციებს.

სტრუქტურის მუშაობის ასახსნელად, განვიხილოთ IoT მოწყობილობა, რომელსაც ჩვენ აღვნიშნავთ, როგორც ID_i-ის, სადაც i მოწყობილობის ნომერია. ნებისმიერი შეტყობინებისთვის, რომელსაც ID_i აგზავნის ქსელში, სტრუქტურა ჯერ ამოწმებს, არის თუ არა ის რეგისტრირებული. სერვერებზე დარეგისტრირების მოთხოვნა გენერირდება, თუ ID_i არ არის რეგისტრირებული. ამის შემდეგ, სტრუქტურა ამოწმებს, არის თუ არა ID_i სანდო (ანუ ატესტირებულია თუ არა) და აგრძელებს შემდეგნაირად:

- თუ ID_i არ არის ატესტირებული, ის აგენერირებს HAtt-ზე დაფუძნებულ ატესტაციის პროცედურას ID_i -სთვის.
  - თუ ის გაივლის პროცედურას, სტრუქტურა მას სანდო იზოლაციის დონეს მიაკუთვნებს;
  - მარცხის შემთხვევაში, სტრუქტურა მას დაუცველი იზოლაციის დონეს მიაკუთვნებს.
- თუ ID_i ატესტირებულია, სტრუქტურა მას ქსელის სანდო იზოლაციის დონეს მიაკუთვნებს.

დაბოლოს, მას შემდეგ, რაც ID_i ჩამოთვლილია სანდო ან დაუცველ დონეზე, სტრუქტურა მუდმივად აკონტროლებს მის ქცევას. თუ ID_i ავლენს მავნე ქცევას, ის გამოცხადებულია კომპრომეტირებულად და შემდეგ გადადის ქსელის კომპრომეტირებული იზოლაციის დონეზე. ამ ეტაპზე, ყველა შეტყობინება, რომელსაც ID_i აგზავნის, იბლოკება მანამ, სანამ არ მოხდება მისი ატესტაცია თავიდან, იმავე პროცედურის მიხედვით. გასათვალისწინებელია, რომ ატესტაცია ხორციელდება ვირტუალურ მანქანაზე, რომელიც გულისხმობს SFV-ის გამოყენებას შემოთავაზებულ სქემაში.

5.4. მახასიათებლების ანალიზი

ეს პარაგრაფი განიხილავს შემოთავაზებულ სტრუქტურას მისი ზემოაღნიშნული მიზნების მიღწევისა და მავნე პროგრამის გავრცელების კონტროლის თვალსაზრისით.

5.4.1. ძირითადი მიზნები

შემოთავაზებული სტრუქტურის გამოყენებით მიიღწევა შემდეგი მიზნები:

მასშტაბურობა: ნახ. 5.2 გვიჩვენებს, რომ არა მხოლოდ ქსელის ფუნქციები, არამედ უსაფრთხოების ფუნქციებიც ვირტუალიზებულია და განლაგებულია ვირტუალურ მანქანებზე გამოყოფილი ტექნიკის ნაცვლად. ამრიგად, ქსელი უფრო რთული და ჰეტეროგენული ხდება და ქსელის SW არ არის საკმარისი B5G ქსელებისთვის. შემოთავაზებულ სტრუქტურაში, ეს საკითხი მოგვარებულია ვირტუალური უსაფრთხოების ფუნქციების განლაგებით ვირტუალურ მანქანებზე. ამრიგად, უსაფრთხოების მრავალი ფუნქცია (ჰეტეროგენული მოწყობილობების მხარდაჭერა) შეიძლება გაშვებულ იქნეს ერთ სერვერზე. უფრო მეტიც, ბლოკჩეინში მრავალი განაწილებული სერვერის არსებობა კიდევ უფრო ზრდის მასშტაბურობას.

უსაფრთხოება: შემოთავაზებულ სტრუქტურაში, სერვისის პროვაიდერი მასპინძლობს ვირტუალურ მანქანებს ქსელისა და უსაფრთხოების სხვადასხვა ფუნქციისთვის. შესაბამისად, მას უფრო მეტი კონტროლი აქვს ამ სერვისების განხორციელებასა და შენარჩუნებაზე. ერთ-ერთი ასეთი მაგალითია ის, რომ თუ სერვისის პროვაიდერი აღმოაჩენს რაიმე დაუცველობას უსაფრთხოების ფუნქციაში, მას შეუძლია მარტივად გამოიყენოს პატჩი და/ან განაახლოს უსაფრთხოების ფუნქცია. უფრო მეტიც, რადგან ბევრი IoT მოწყობილობა შეზღუდულია რესურსების თვალსაზრისით, შემოთავაზებული სტრუქტურა გამოიყენება გამოთვლითი სირთულის გადატვირთვისთვის პერიფერიული მოწყობილობიდან ღრუბელში. ამ შემთხვევაში, ჩვენ ვირტუალიზაცია მოვახდინეთ ატესტაციის პროცედურის ორი ძირითადი მიზნის მისაღწევად: პირველი, უსაფრთხოების ფუნქციებზე მეტი კონტროლის უზრუნველყოფა სერვისის პროვაიდერისთვის და მეორე, ჰეტეროგენული მოწყობილობების ფართო სპექტრის მხარდაჭერა, მათ შორის, რესურსებით შეზღუდული მარტივი IoT მოწყობილობებისთვის.

მოქნილობა: შემოთავაზებულ SFV სტრუქტურაში, სერვისის პროვაიდერებს შეუძლიათ ვირტუალური უსაფრთხოების ფუნქციების გაშვება სხვადასხვა სერვერზე ან მათი გადაადგილება საჭიროებისამებრ, როდესაც მოთხოვნა იცვლება. ეს არა მხოლოდ საშუალებას აძლევს სერვისის პროვაიდერებს, უფრო სწრაფად მიაწოდონ სერვისები და აპლიკაციები, არამედ შეიძლება გამოყენებულ იქნეს, როგორც დაბალი რისკის საშუალება პოტენციური ახალი სერვისის ფასეულობის შესამოწმებლად.

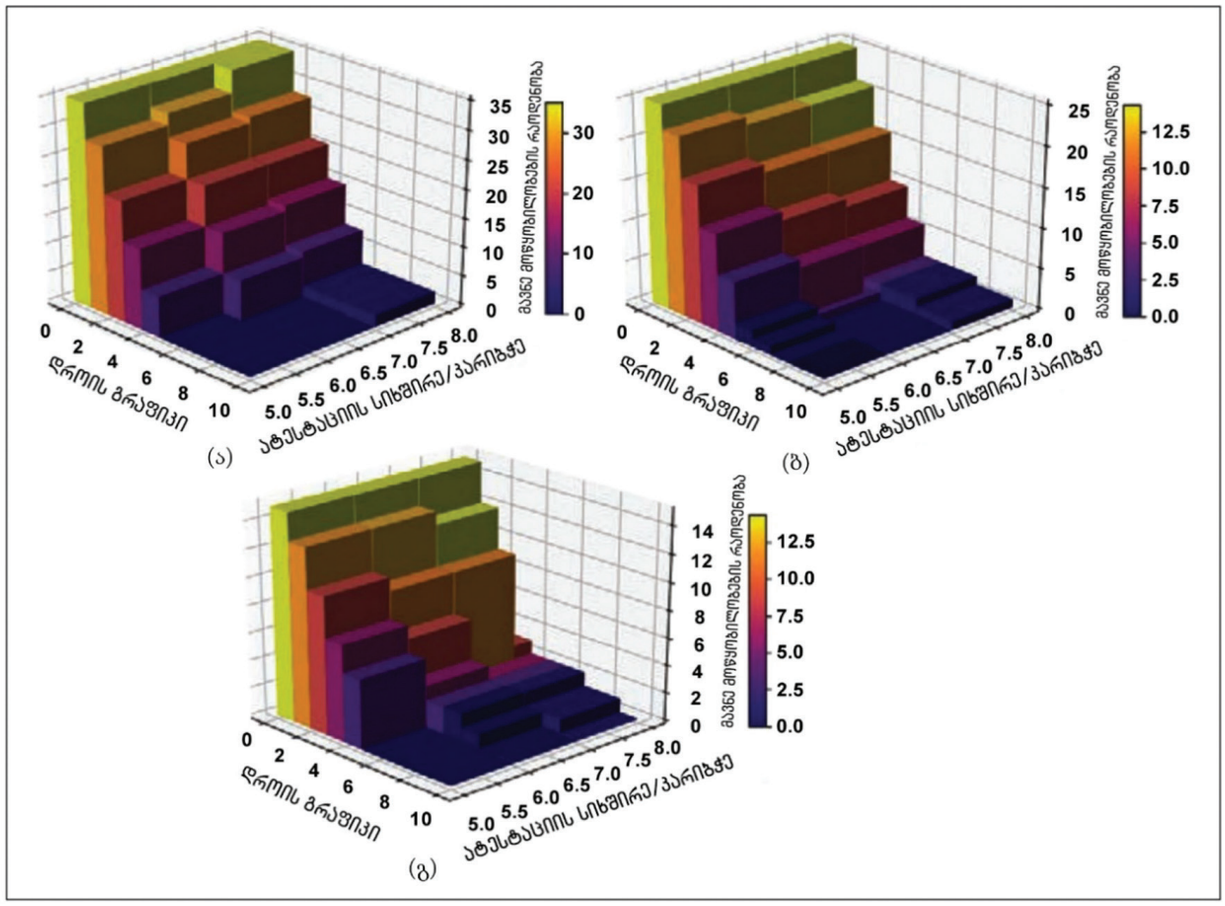
ღირებულება: სერვისის პროვაიდერებს ახლა შეუძლიათ უსაფრთხოების ფუნქციების გაშვება ჩვეულებრივ აპარატურაზე და არა სპეციალურ აპარატურაზე, SFV-ის გამოყენებით. გარდა ამისა, უსაფრთხოების ფუნქციების ვირტუალიზაციით, რამდენიმე ფუნქციის გაშვება შესაძლებელია ერთ სერვერზე. ეს იწვევს ფიზიკური ტექნიკის მოცულობის შემცირებას, რაც იძლევა რესურსების კონსოლიდაციის საშუალებას, ამას კი საბოლოო ჯამში მივყავართ ფიზიკური სივრცის, ენერგეტიკული და მთლიანი ხარჯების დაზოგვამდე.

5.4.2. მავნე პროგრამების კონტროლი

შემოთავაზებული სტრუქტურის ეფექტიანობის შესაფასებლად, ჩატარდა სიმულაციები პითონზე (Python) დაფუძნებული დისკრეტული ხდომილებების სიმულატორის გამოყენებით. გარდა ამისა,

შეფასებული იქნა სამი სცენარი, დაწყებული კომპრომეტირებული მოწყობილობების ფიქსირებული პროცენტით. ყველა სიმულაცია გაშვებული იყო 10 წამის განმავლობაში, 5-7 წამის ატესტაციის დროის პერიოდის (t_a) გამოყენებით, რაც მიუთითებს იმაზე, რომ IoT მოწყობილობები სკანირებულია მავნე პროგრამებზე ყოველ 5-7 წამში ერთხელ. შედეგები თითოეული სცენარისთვის მიღებულ იქნა საშუალოდ, 100 სიმულაციის გამოყენებით. გასათვალისწინებელია ის გარემოება, რომ ამ სიმულაციებში, ჩვენი ვარაუდით, მოწყობილობების 10 პროცენტი მხარდაჭერილია უსაფრთხოების პატჩებით, ხოლო დანარჩენი 90 პროცენტი (თუ ინფიცირებულია) საჭიროებს ვირტუალურ პატჩებს. დასკვნების მიხედვით, თუ მოწყობილობაში გამოყენებულია ვირტუალური პატჩები, ის არ ითვლება ინფიცირებულად.

შემთხვევა 1: პირველი სცენარისთვის, ჩვენ ვივარაუდეთ, რომ მოწყობილობების 70 პროცენტი იყო ინფიცირებული მავნე პროგრამით, ანუ 35 მოწყობილობა 50-დან. ნახ. 5.4ა აჩვენებს, რომ ჩვენს სტრუქტურას შეუძლია მნიშვნელოვნად შეამციროს მავნე პროგრამების გავრცელება მოწყობილობებზე შედარებით მოკლე დროში (10 წმ). როგორც ვხედავთ, ინფიცირებული მოწყობილობების რაოდენობა 35-დან 0-მდე ეცემა, როდესაც t_a = 5 წმ. ანალოგიურად, t_a = 6 წმ-სთვის, ინფიცირებული მოწყობილობების რაოდენობა შემცირდა 35-დან 0-მდე, ხოლო t_a = 7 წმ-სთვის, ინფიცირებული მოწყობილობების რაოდენობა შემცირდა 35-დან 2-მდე 10 წამში.



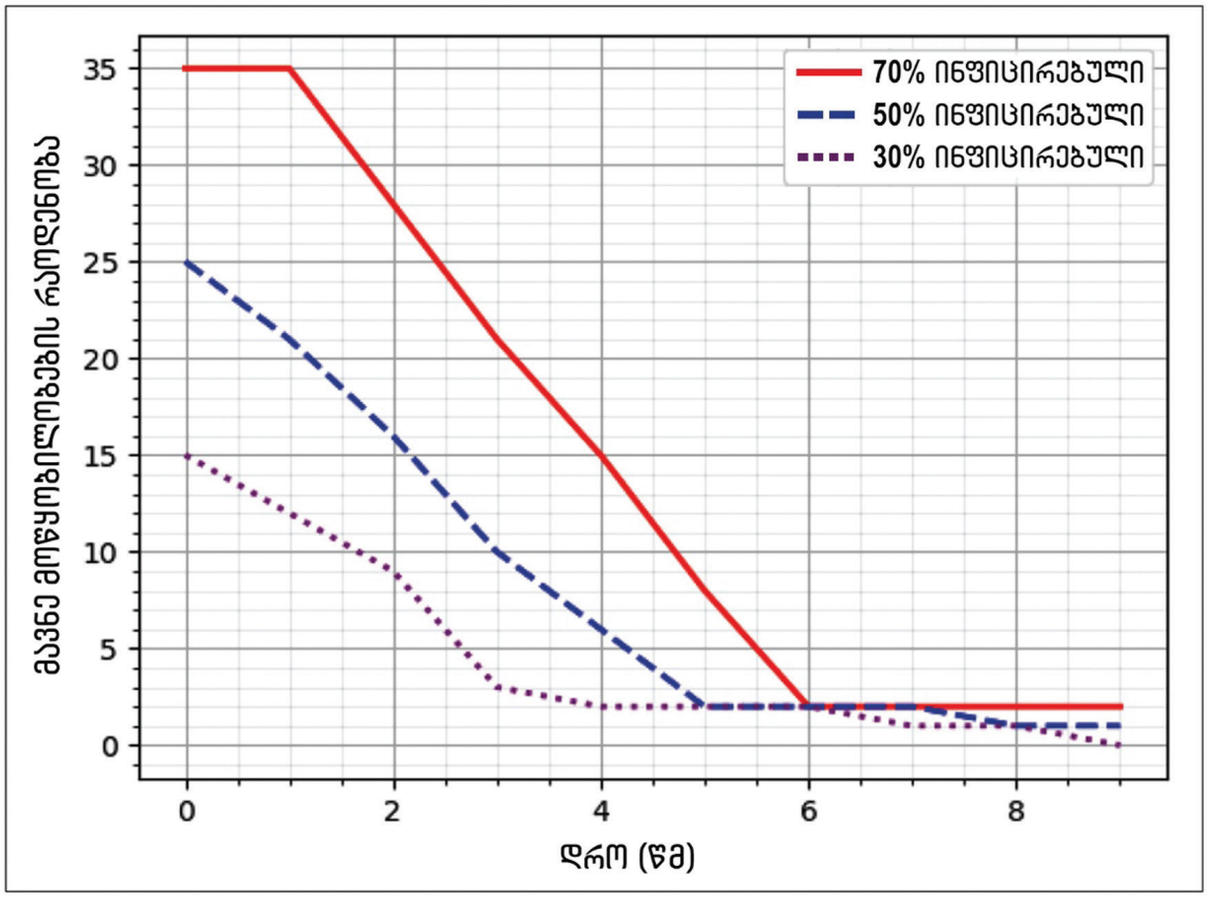
ნახ. 5.4. მავნე პროგრამების კონტროლი შემოთავაზებული უსაფრთხოების სტრუქტურის გამოყენებით: ა) მავნე მოწყობილობების 70 პროცენტი; ბ) მავნე მოწყობილობების 50 პროცენტი; გ) მავნე მოწყობილობების 30 პროცენტი

შემთხვევა 2: მეორე სცენარისთვის, ჩვენ ვივარაუდეთ, რომ მოწყობილობების 50 პროცენტი, ანუ 25 მოწყობილობა, თავდაპირველად დაინფიცირებული იყო მავნე პროგრამით. ნახ. 5.4ბ აჩვენებს,

რომ ჩვენს სტრუქტურას შეუძლია მნიშვნელოვნად შეამციროს მავნე პროგრამების გავრცელება მოწყობილობებზე მოკლე დროში. როგორც ვხედავთ, ინფიცირებული მოწყობილობების რაოდენობა შემცირდა 25-დან 0-მდე, როდესაც t_a = 5 წმ. ანალოგიურად, t_a = 6 წმ-სთვის, ეს რიცხვი 25-დან ნულამდე შემცირდა, ხოლო t_a = 7 წმ-სთვის, ინფიცირებული მოწყობილობების რაოდენობა შემცირდა 25-დან 1-მდე 10 წამში.

შემთხვევა 3: მესამე სცენარი მიიჩნევს, რომ მოწყობილობების 30 პროცენტი თავდაპირველად დაინფიცირებულია მავნე პროგრამით (ანუ 15 მოწყობილობა). ნახ. 5.4გ გვიჩვენებს ინფიცირებული მოწყობილობების რაოდენობის მნიშვნელოვან შემცირებას ჩვენი უსაფრთხო სტრუქტურის მეშვეობით, რომელიც იყენებს პატჩებს. ვხედავთ, რომ t_a = 5 წმ-სთვის, ინფიცირებული მოწყობილობების რაოდენობა 15-დან 0-მდე შემცირდა. ანალოგიურად, t_a = (6,7) წმ-სთვის, ინფიცირებული მოწყობილობების რაოდენობა 10 წამში 15-დან შემცირდა 0-მდე.

ატესტაციის სიხშირის მუდმივი სიდიდის შენარჩუნებით 8/კარიბჭეზე, ინფიცირებული მოწყობილობების რაოდენობის შემცირება დროის მიხედვით ნაჩვენებია ნახ. 5.5-ზე. ჩვენ შეგვიძლია დავაკვირდეთ, რომ შემოთავაზებულ სტრუქტურას შეუძლია ეფექტიანად გააკონტროლოს, შეზღუდოს და შეამციროს მავნე პროგრამის გავრცელება. შედეგები აჩვენებს, რომ თავდაპირველად ინფიცირებული IoT მოწყობილობების 70 პროცენტის შემთხვევაშიც კი, რვა წამში ერთხელ ატესტაციის სიხშირით, სტრუქტურა ეფექტიანად ეწინააღმდეგებოდა მავნე პროგრამის გავრცელებას და ზღუდავდა ინფიცირებული მოწყობილობების რაოდენობას, რომელიც შემცირდა 4 პროცენტამდე, საკმაოდ მოკლე დროში – 10 წმ.



ნახ. 5.5. დროის მიხედვით ინფიცირებული მოწყობილობების რაოდენობა ატესტაციის სიხშირით 8/კარიბჭეზე

5.5. მეხუთე თავის დასკვნა

SFV არის თანამედროვე კონცეფცია, რომელიც გვთავაზობს ახალ შესაძლებლობებს 6G ქსელებში უსაფრთხოების გასაუმჯობესებლად და თანმდევი ოვერჰედის შემცირებისთვის. ის ითვალისწინებს უსაფრთხოების თავსებადობის საკითხებს საბოლოო მომხმარებლებსა და სისტემებს შორის უსაფრთხოების ვირტუალიზაციის ფენის უზრუნველყოფით. IoT მოწყობილობების მზარდი რაოდენობით 5G და 6G ქსელებში, მავნე პროგრამა IoT სისტემებში გახდა უსაფრთხოების ერთ-ერთი მთავარი პრობლემა. ეს თავი განიხილავს ამ საკითხს უსაფრთხოების სტრუქტურის შემოთავაზებით, რომელიც იყენებს უსაფრთხოების ფუნქციების SW-ს SFV-ზე დაფუძნებით, რათა თავიდან აიცილოს მავნე პროგრამების გავრცელება და მოახდინოს IoT მოწყობილობების იზოლირება სანდო, დაუცველი და კომპრომეტირებული ქსელის იზოლაციის დონეებზე დისტანციური ატესტაციის საშუალებით. მოწყობილობების იზოლირებისთვის, NFV გამოიყენება თითოეული კატეგორიისთვის ცალკეული ქსელების შესაქმნელად, ხოლო განაწილებული ლეჯერი გამოიყენება თითოეული მოწყობილობის მდგომარეობის შესანახად. IoT მოწყობილობების ჰეტეროგენული ჯგუფის ფარგლებში, თავსებადობის პრობლემების თავიდან ასაცილებლად, გამოიყენება ვირტუალური დისტანციური ატესტაციის პროცედურები. ნაჩვენებია, რომ შემოთავაზებული სტრუქტურა არა მხოლოდ უზრუნველყოფს უკეთეს უსაფრთხოებას, არამედ იწვევს გაუმჯობესებულ მასშტაბურობას, მოქნილობას, ღირებულებას და მავნე პროგრამების კონტროლს. შედეგები აჩვენებს, რომ შემოთავაზებულმა სტრუქტურამ მხოლოდ 10 წამში შეამცირა ინფიცირებული მოწყობილობების რაოდენობა 66 პროცენტით.

თავი 6. ღრმა სწავლებაზე დაფუძნებული საფრთხეების გამოვლენის სქემა საგნების ინდუსტრიული ინტერნეტისთვის

6.1. შესავალი

IIoT არის დაკავშირებული ინტელექტუალური მოწყობილობების გამოყენება ინდუსტრიულ აპლიკაციებში ისეთი მიზნებისთვის, როგორიცაა ავტომატიზაცია, დისტანციური მონიტორინგი და პროფილაქტიკური მომსახურება. IIoT არის საგნების ინტერნეტის, ანუ IoT-ის უფრო სრულყოფილი ვერსია, რომელიც ქმნის დაკავშირებული მოწყობილობების სფეროს კომერციულ და სამომხმარებლო აპლიკაციებში. IIoT-ის გამოყენების შემთხვევაში, ინტელექტუალური მოწყობილობები შეიძლება განთავსდეს სამშენებლო მანქანებში, მიწოდების ჯაჭვის რობოტიკაში, მზისა და ქარის ენერგეტიკაში, სასოფლო-სამეურნეო სენსორულ სისტემებში, ჭკვიან სარწყავ სისტემებში და სხვა. ამ IIoT აპლიკაციებს ერთი რამ აქვთ საერთო: ისინი განლაგებულია რთულ და გამოწვევებით სავსე გარემოში. მოსალოდნელია, რომ IIoT გახდება B5G/6G ქსელების შემადგენელი ნაწილი და ამ ქსელების კონცეფცია ფართოდ იქნება გამოყენებული IIoT მოწყობილობების შესაქმნელად.

IIoT ეყრდნობა შეგროვებული ინდუსტრიული მონაცემების დიდ მოცულობას პრობლემების აღმოსაფხვრელად, წარმადობის შეფერხებების იდენტიფიცირებისთვის და მავნე ქცევის გამოსავლენად, რათა მიღწეულ იქნეს ფიზიკურ სამყაროზე ეფექტიანი კონტროლი. დროთა განმავლობაში, IIoT თანდათან იქნება გამოყენებული ეროვნულ კრიტიკულ ინფრასტრუქტურულ სისტემებში, როგორც ნავთობქიმიური ინდუსტრიის, ელექტროქსელების, წყლის კონსერვაციის, ბირთვული ენერგიისა და ტრანსპორტის მხარდამჭერი. ამასთან, IIoT-ის სწრაფ განვითარებას თან ახლავს კიბერთავდასხმების გაჩენა კრიტიკულ ინფრასტრუქტურაზე. ქსელზე ტრადიციული თავდასხმების გარდა, APT თავდასხმებიც იზრდება. APT არის მდგრადი და მიზანმიმართული კიბერთავდასხმა, რომლის დროსაც თავდამსხმელი იძენს წვდომას კრიტიკულ ინფრასტრუქტურულ სისტემებზე და რჩება შეუმჩნეველი, სანამ სამიზნე არ განადგურდება. APT სერიოზულ საფრთხეს უქმნის კრიტიკულ ინფრასტრუქტურულ სისტემებს და უკვე მრავალი ავარია გამოიწვია.

APT თავდასხმები სერიოზული საფრთხეა კრიტიკული ინფრასტრუქტურის სისტემებისთვის. APT-ის გამოვლენის ამჟამინდელი მეთოდები ძირითადად ეფუძნება განაწილებულ გამოთვლებს, დიდ მონაცემებს, ღრუბლოვან გამოთვლებსა და მონაცემთა მოპოვების ტექნოლოგიებს, როგორიცაა: მასპინძელი მავნე კოდის ანომალიის გამოვლენა, სენდბოქსის (sandbox) მავნე კოდის ანომალიის გამოვლენა, კორელაციის ანალიზი, ტრაფიკის ანომალიის გამოვლენა და ქსელის ყოვლისმომცველი ხელში ჩაგდება. ტრადიციული მეთოდები რთული გამოსაყენებელია IIoT-სთვის. ლიტერატურაში შემოთავაზებულია APT-ის გამოვლენის მეთოდი, რომელიც აანალიზებს სოციალური ქსელის უსაფრთხოების მოვლენებს. ღრუბლოვანი გამოთვლების ქსელური ტრაფიკის ანალიზთან კომბინაციით, შემუშავებულია საპირისპირო ნაკადის გამოვლენის მოდელი, რომელიც ეფუძნება ტრაფიკის ცვლილებებს. მთავარი იდეა არის აპლიკაციის კონტეინერის შექმნა, რომელიც ახორციელებს პროგრამას APT თავდასხმების აღმოსაჩენად, ქსელის ბოლო წერტილების ქცევის მონიტორინგით. გარდა ამისა, თავდაცვის არქიტექტურა, მათ შორის APT კარიბჭის ამოცნობა და APT მართვის კონსოლი, შემუშავებულია მასპინძელი სისტემის გარემოს, აპლიკაციის გარემოს, საკომუნიკაციო გარემოს, მონაცემთა გარემოს, ტრაფიკის მახასიათებლებისა და ქსელის პროტოკოლის მახასიათებლების მონიტორინგისა და ანალიზისთვის. APT-ის გამოვლენის

ზემოთ ნახსენებ მეთოდებს აქვთ გარკვეული ვალიდობა, მაგრამ ისინი ძირითადად გამოიყენება APT თავდასხმებისთვის მცირე ხანგრძლივობით და ფიქსირებული თავდასხმის შაბლონებით, ხოლო APT თავდასხმები IIoT-ში ჩვეულებრივ, დიდი მასშტაბითა და ხანგრძლივობით ხასიათდება. ამრიგად, აღმოჩენის არსებულ მეთოდებს არ შეუძლია გამოვლენის მაღალი სიზუსტის უზრუნველყოფა IIoT-ში გამოყენებისას.

AI-ის და IoT-ის ინტეგრაცია ამჟამად არის კვლევის ცხელი თემა. მათი ერთობლიობა წარმოქმნის მძლავრ ტექნოლოგიას, საგნების ხელოვნურ ინტელექტს – AIoT-ს, რომელიც მოწყობილობებს საშუალებას აძლევს, შეაგროვონ მონაცემები და გააანალიზონ ისინი, რათა მიიღონ ადამიანის მსგავსი გადაწყვეტილებები. AIoT-ის პოპულარობიდან გამომდინარე, APT-ები და „ნულოვანი დღის დაუცველობა“ გამოჩნდა ზოგიერთ მნიშვნელოვან IIoT-ში (ნულოვანი დღის დაუცველობა არის დაუცველობა სისტემაში ან მოწყობილობაში, რომელიც გამოვლენილია, მაგრამ ჯერ არ არის პატჩით შესწორებული). AI-ის, განსაკუთრებით DL-ის, ტრადიციულ მეთოდებთან შედარებით აქვს უპირატესობა ასეთი თავდასხმების გამოვლენასა და მისგან დაცვაში. კრიტიკულ ინფრასტრუქტურულ სისტემებში IIoT-სთვის შესაფერისი APT-ის გამოვლენის მეთოდის შესთავაზებლად, ეს თავი იკვლევს DL-ზე დაფუძნებულ APT-ის პროაქტიული გამოვლენის სქემას IIoT-ში, მასში APT თავდასხმების მახასიათებლებზე დაყრდნობით, როგორიცაა თავდასხმების გრძელი მიმდევრობა და გრძელვადიანი თავდასხმის ხანგრძლივობა. APT თავდასხმების მიმდევრობის გამოვლენისთვის გამოყენებულია მიმდევრობის დამუშავების BERT მოდელი DL-ზე დაფუძნებული მეთოდების არეალიდან. ჩვენ ასევე ვახდენთ APT თავდასხმების მიმდევრობის მონაცემების ოპტიმიზაციას, რათა მოხდეს მისი ნორმალიზება და უფრო ცხადი გავხადოთ ის ორიგინალური მონაცემების ნებისმიერი შინაარსის განადგურების გარეშე, რაც უზრუნველყოფს დატრენინგებული მოდელის ეფექტიანობას გრძელვადიანი თავდასხმის მიმდევრობის გამოვლენის პროცესში.

ეს თავი ორგანიზებულია შემდეგნაირად: პარაგრაფი 6.2 აღწერს APT თავდასხმებს IIoT-ში, ხოლო პარაგრაფი 6.3 წარმოგვიდგენს ღრმა სწავლების მეთოდს IIoT-ში APT-ის პროაქტიული გამოვლენისთვის. ამის შემდეგ, პარაგრაფში 6.4 მოყვანილია ექსპერიმენტული ანალიზი, ხოლო ბოლო ნაწილი აჯამებს მეექვსე თავს.

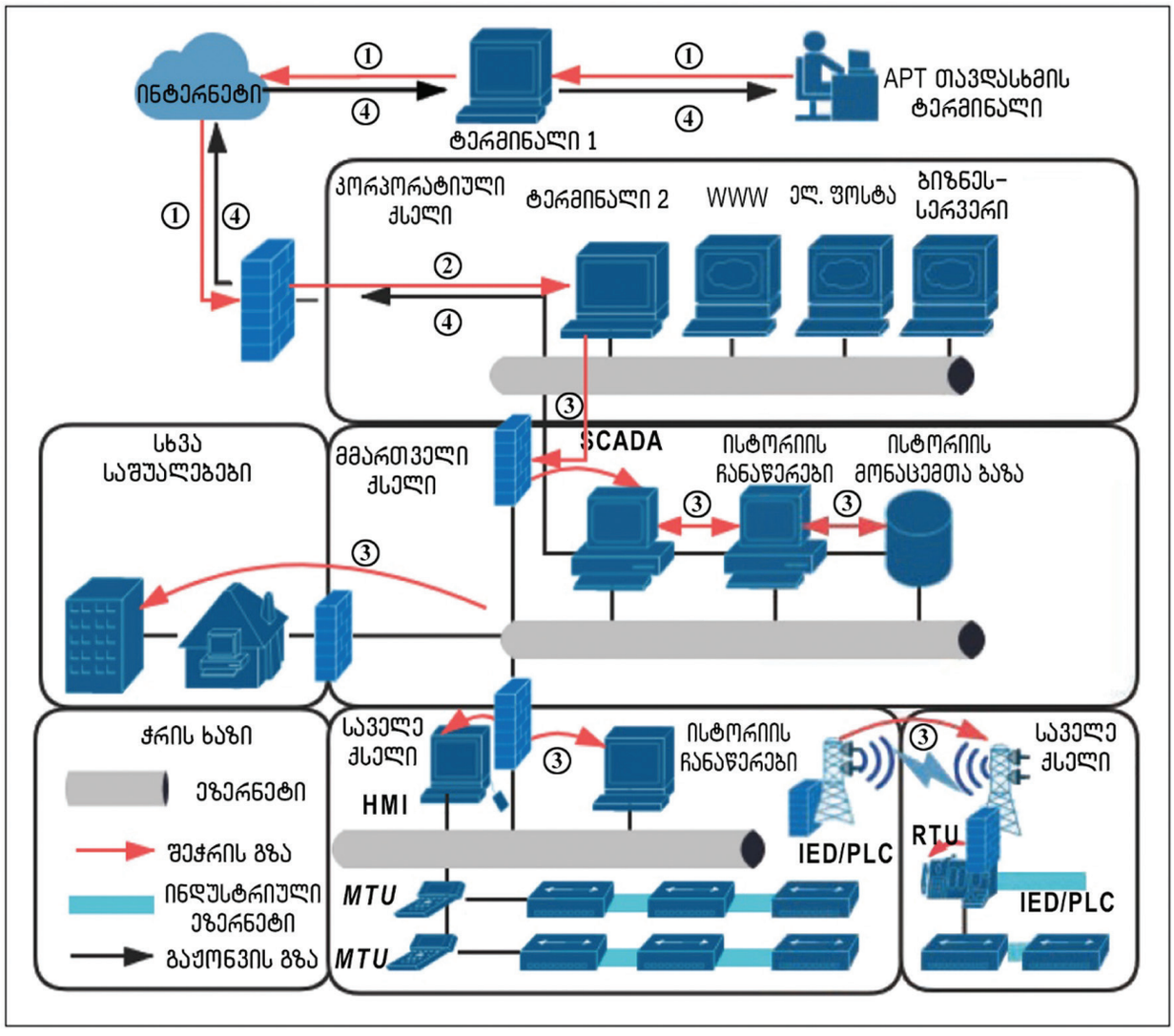
6.2. APT თავდასხმების აღწერა IIoT-ში

ამ პარაგრაფში ჩვენ მოკლედ აღვწერთ APT თავდასხმებს IIoT-ში; APT თავდასხმის სრული სასიცოცხლო ციკლი IIoT-ში ნაჩვენებია ნახ. 6.1-ზე. თავდასხმის პროცესი შეიძლება დაიყოს შემდეგ ხუთ ეტაპად: მონაცემთა შეგროვება, გეგმის ფორმულირება, პრივილეგიების ესკალაცია და შიგნით შეღწევა, უფლებამოსილების შენარჩუნება და თვალთვალის საწინააღმდეგო ქმედებები, მიზნის განხორციელება და კვალის გაწმენდა. ჩვენ თითოეულ ეტაპს შემდეგნაირად აღვწერთ:

პირველი ეტაპი არის მონაცემთა შეგროვება, რომლის დროსაც ინფორმაცია გროვდება IIoT ქსელში ყველა ქსელის სკანირებითა და გამოვლენით, რომელთა შორისაა: კორპორატიული ქსელი, მმართველი ქსელი და საველე ქსელი. მონაცემთა შეგროვება ხდება მთელი თავდასხმის განმავლობაში. მიზანია, თავდამსხმელმა მოიპოვოს ისეთი ინფორმაცია, როგორიცაა აქტივების, მომხმარებლის, მომწოდებლის ინფორმაცია, საფოსტო ყუთები და ანგარიშის ნომრები სამიზნე ქსელში. ყველა ეს ქმედება ემსახურება თავდასხმის ეფექტიანი გეგმის შედგენის მომზადებას.

მეორე ეტაპი არის გეგმის ფორმულირება. მას შემდეგ, რაც IIoT ქსელის ძირითადი ინფორმაცია და ტოპოლოგიური სტრუქტურა აითვისება შეგროვებული ინფორმაციის მეშვეობით, ჰაკერი იღებს წვდო-

მას IIoT ქსელში. ეფექტიანი თავდასხმის გეგმა ჩამოყალიბებულია ელექტრონული ფოსტის, მყისიერი შეტყობინებების, სოციალური ქსელების ან აპლიკაციის სისუსტეების გამოყენებით IIoT ქსელში მოწყობილობებზე ან სერვერებზე თავდასხმისთვის, როგორც თავდასხმის წინასწარი ჩანაწერი.



ნახ. 6.1. IIoT-APT თავდასხმის სტრუქტურა (აკრონიმები მოცემულია წიგნის ბოლოს, განყოფილებაში: აბრევიატურები და აკრონიმები)

მესამე ეტაპი არის პრივილეგიების ესკალაცია და შიდა შეღწევა, რაც IIoT-ზე თავდასხმების მთავარი მიზანია. ჰაკერები, პირველ რიგში, იყენებენ SW-ის ან მენეჯმენტის დაუცველობას, როგორიცაა ვებსერვისები, ელექტრონული ფოსტა ან ბიზნესსერვისები კორპორაციულ IIoT ქსელში მავნე კოდის ჩასანერგად, რომელთა მაგალითებია: ჩამწერები, ტროას ცხენები, პაროლის გატეხვა და ფაილების შეგროვების პროგრამები. სანამ ეს ოპერაცია წარმატებულია, ჰაკერებს შეუძლიათ იმალებოდნენ კორპორაციულ ქსელში, რათა შეაგროვონ სულ უფრო და უფრო მეტი ინფორმაცია. მოგვიანებით მოსახერხებელი ხდება ჰორიზონტალური შეღწევადობის გამოყენება კორპორაციულ ქსელში კონფიგურაციის ფაილის და Terminal2 ბიზნესინტერფეისის მოსაძებნად, ამით კი IIoT მმართველ ქსელში შესვლა. ჰაკერები გატეხენ დომენის მმართველ სერვერს, როგორც თავდასხმის ფოკუსს. დომენის მართვის სერვერის უფლებამოსილების მოპოვების შემდეგ, ჰაკერს შეუძლია თავისუფლად შევიდეს IIoT საველე ქსელში და შემდგომ გააკონტროლოს წარმოების აღჭურვილობა.

მეოთხე ეტაპი არის უფლებამოსილების შენარჩუნება და თვალთვალის საწინააღმდეგო ქმედებები. IIoT-ში კორპორაციული, მმართველი ან საველე ქსელის მონაცემების მოპარვის პროცესი რთული და შრომატევადია. მოპოვებული ნებართვების შესანარჩუნებლად, ჰაკერები შეიმუშავებენ შესაფერის მეთოდებს, რათა თავიდან აიცილონ თვალთვალი და დარჩნენ ღრმად დამალული, როგორიცაა თვითნაკეთი მკვლელობის საწინააღმდეგო რადიო წვდომის ტექნოლოგიების (RAT) კლასტერული სისტემის ან Cobalt Strike-ის გამოყენება. მონაცემთა გადაცემისას, ისეთი მეთოდები, როგორიცაა ბაიტის გაყოფა და გაერთიანება, ასევე შეიძლება გამოყენებულ იქნეს შეგროვებული ინფორმაციის ნელა გადასაცემად, რათა თავიდან იქნეს აცილებული ანომალიური ტრაფიკის გამოვლენა ანალიზის სპეციალური ხელსაწყოებით. როგორც უკვე აღვნიშნეთ, ყალბი პირადობისა და პლაცდარმების გამოყენება, ასევე ხელს შეუშლის მთელი APT თავდასხმის მიკვლევადობას მაშინაც კი, როდესაც თავდასხმა აღმოჩენილია.

დასკვნითი ეტაპია მიზნის განხორციელება და კვალის გაწმენდა, ანუ კორპორაციული, მმართველი და საველე ქსელებიდან კონფიდენციალური მონაცემების უკანონო გადატანა ჰაკერის მიერ კონტროლირებად გარე სისტემაში. ჰაკერი იყენებს მოპოვებულ მონაცემებს ან მასთან დაკავშირებულ ალგორითმებს, რათა აღმოაჩინოს ფესვეული (root) მომხმარებლის კომპიუტერი, შეგროვებული ქსელის ტრაფიკის ინფორმაციისა და სამიზნე სისტემის ჟურნალის ფაილებიდან. ფესვეული მომხმარებლის ინფორმაციითა და ფესვეული ნებართვებით, ჰაკერებს შეუძლიათ მიიღონ წვდომა მონაცემთა ცენტრში ან მისცენ ინსტრუქციები სხვა მანქანებს. მონაცემთა ცენტრის შიგნით არსებული ძირითადი მონაცემები თავდამსხმელს დაშიფრული არხებით გადაეცემა. საბოლოოდ, წვდომის კვალი, ჟურნალი და სხვა დაკავშირებული ინფორმაცია გასუფთავებულია.

უნდა აღინიშნოს, რომ ქსელის ტრადიციულ თავდასხმებთან შედარებით, APT თავდასხმებს აქვთ უნიკალური მახასიათებლები:

თვისება 1: APT თავდასხმები IIoT-ზე იყენებს მთავრობის ან თუნდაც, მთელი ქვეყნის ძალას. მიუხედავად იმისა, თუ რამდენი ცოცხალი ძალა და რესურსია ჩართული, ასეთი თავდასხმები არ წყდება მანამ, ვიდრე მიზანს არ მიაღწევენ. ეს ქმნის დიდ პრობლემას თავდასხმების თავიდან ასაცილებლად.

თვისება 2: IIoT-ზე APT თავდასხმების დროს ჰაკერები ჩუმად და დაფარულად არიან დიდი ხნის განმავლობაში, ყველა ეტაპზე. ეს ნიშნავს, რომ არსებული შეჭრის გამოვლენის SW და ანტივირუსული SW ვერ ახერხებენ APT თავდასხმების იდენტიფიცირებას მონაცემთა შესატყვისი ანალიზისა და ანომალიების გამოვლენის საშუალებით.

6.3. ღრმა სწავლებაზე დაფუძნებული, APT-ის პროაქტიული გამოვლენა IIoT-ში

ამ პარაგრაფში განხილულია IIoT-ში APT-ის პროაქტიული გამოვლენის DL მეთოდი. ანომალიის გამოვლენა, რომელიც დაფუძნებულია ზედამხედველობის გარეშე სწავლებაზე, ძალიან პოპულარულია შემდეგი მიზეზების გამო: პირველი, IIoT-ში ზოგიერთ ნორმალურ და არანორმალურ მონაცემს არ აქვს მკაფიო საზღვრები; მეორე, შეგროვებული IIoT მონაცემები ასევე შეიცავს ხმაურს, რომელიც ძნელია განასხვაო ანომალიებისგან; მესამე, დროთა განმავლობაში, ნორმალური ქცევა შეიძლება შეიცვალოს; დაბოლოს, ეტიკეტირებული მონაცემების მიღება რთულია. ზედამხედველობის გარეშე სწავლების პოპულარულ მეთოდებს მიეკუთვნება სტატისტიკაზე დაფუძნებული ანომალიის გამოვლენა, სიმკვრივეზე დაფუძნებული ანომალიის გამოვლენა, კლასტერზე დაფუძნებული ანომალიის გამოვლენა, ანომალიის გამოვლენა ერთი კლასის SVM (One-Class SVM) მეთოდით და ანომალიის გამოვლენა იზო-

ლირებული ტყის ინტეგრირებული სწავლების მეთოდის გამოყენებით. რეალურ პროექტებში, თუ არსებობს შედარებით მცირე, წინასწარ მარკირებული მონაცემები, შეიძლება გამოყენებულ იქნეს ზედამხედველობის გარეშე სწავლების მეთოდები. თუმცა, ვინაიდან ამ თავში ეტიკეტირებული მონაცემები მოდის კერძო ენერგოსისტემიდან, ჩვენ ქვემოთ გამოვიყენებთ ზედამხედველობითი სწავლების მეთოდს.

6.3.1. APT თავდასხმების მიმდევრობის ანალიზი

როგორც ზემოთ მოყვანილი ანალიზიდან ჩანს, APT თავდასხმები IIoT-ში ხასიათდება გრძელვადიანი მდგრადობით და შეიძლება რამდენიმე წუთიდან რამდენიმე წლამდე მერყეობდეს. ამიტომ, APT თავდასხმების მიმდევრობა არის უცნობი მიმდევრობა ცვლადი სიგრძით. თავდასხმის დასასრულებლად, IIoT-ის APT თავდამსხმელმა უნდა დააკავშიროს ტრადიციული ქსელის თავდასხმები სხვადასხვა მოწინავე მეთოდთან. დაკავშირებული აქტივობები, რომლებიც საფუძვლად უდევს APT თავდასხმებს, არის მიზანმიმართული და უწყვეტი, მაგრამ ისინი შეიძლება იყოს არაპირდაპირი, როგორიცაა: ინფორმაციის შეგროვება, გეგმის ფორმულირება, პრივილეგიების ესკალაცია და ა. შ. IIoT-სთვის არსებული APT მოვლენების ანალიზზე დაყრდნობით, IIoT-ის ქცევითი მონაცემები შეიძლება დაიყოს ხუთ კატეგორიად: ნორმალური მონაცემები, მონიტორინგისა და გამოვლენის აქტივობები, პრივილეგიების ესკალაცია, ბრძანების ოპერაცია, თავდასხმა და ქურდობა.

ნორმალური მონაცემები: კორპორაციულ, მმართველ და საველე ქსელებში, ინდუსტრიული კონტროლის ადგილი, აპარატის სტატუსი და ა. შ. უკვე იმყოფება ან უნდა შევიდეს APT თავდასხმის მდგომარეობაში. წყვეტილი ან ინკუბაციური თავდასხმის პერიოდში, ქსელს შეუძლია განახორციელოს ნორმალური კომუნიკაცია რეალურ დროში და მიიღოს მოთხოვნები ბრაუზერის მეშვეობით. მაგალითად, მას შეუძლია მიიღოს HTTP მოთხოვნის შეტყობინებები უსაფრთხო და საიმედო მონაცემებით.

მონიტორინგისა და გამოვლენის აქტივობები: თავდამსხმელმა უნდა შეაგროვოს დიდი რაოდენობით ინფორმაცია სამიზნე სისტემის შესახებ, მათ შორის, მასპინძელი პორტის კომუნიკაციის სტატუსი კორპორაციულ, მმართველ და საველე ქსელებში, ასევე მასპინძელი ქსელის სტატუსი, მონაცემთა ნაკადი, ქსელში ინფორმაციის გადაცემის სტატუსი და ა. შ. სასარგებლო მონაცემების მისაღებად გამოიყენება პორტის სკანირება, კოდის ანალიზი, სტრუქტურირებული შეკითხვების ენის (SQL) განცხადების ამოცნობა და სხვა მეთოდები. ამ საფეხურზე ჩვენ ამ აქტივობების იდენტიფიცირებას ვახდენთ აუდიტორული სისტემის ჟურნალის ანალიზით, ხოლო ასეთი მონაცემების იდენტიფიცირება და აღრიცხვა ხდება ქსელის ტრაფიკის ანალიზის, თავდაცვის სისტემის სიგნალიზაციის და ა. შ. მეშვეობით.

პრივილეგიების ესკალაცია: აღნიშნული მოიცავს ჰორიზონტალური და ვერტიკალური პრივილეგიების გაძლიერებას. ჰორიზონტალური პრივილეგიების ესკალაცია ნიშნავს, რომ თავდამსხმელმა მიიღო გარკვეული მომხმარებლისგან წვდომის ნებართვა, მაგრამ მიღებული ინფორმაცია არ არის საკმარისი. ამ დროს, თავდამსხმელი შეეცდება გამოიყენოს სხვადასხვა გაანალიზებული დაუცველობა და მოიპოვოს სხვა მომხმარებლების ინფორმაცია ზუსტი ფიშინგის საშუალებით. პრივილეგიების ვერტიკალური ესკალაციით, თავდამსხმელი აფართოებს ერთი მომხმარებლის პრივილეგიებს ადმინისტრატორის პრივილეგიებამდე, რათა სრულად გააკონტროლოს სისტემა.

ბრძანების ოპერაცია: იქნება ეს საველე, მმართველი თუ კორპორაციული ქსელი, თავდამსხმელი ასრულებს ფაილებთან დაკავშირებულ ოპერაციებს. ვინაიდან სერვერის სისტემა შეიძლება დაფუძნებული იყოს Linux-ზე, მასპინძელ სისტემაში არსებულ დირექტორიებსა და პროგრამებს, მონაცემებს, სე-

რვისებს, მოწყობილობებს, დრაივერებს და შემავალ/გამომავალ ფაილებს აქვთ შესაბამისი მფლობელის წაკითხვის, ჩაწერისა და შესრულების ნებართვები. თავდამსხმელის მიერ ამ ბრძანებების შესრულება დაკავშირებულია უკანონო წვდომასთან, დისტანციურ მანქანებზე უკანონო ოპერაციებთან და ასეთი ტიპის ბრძანების ოპერაციის მონაცემები შეიძლება ჩაიწეროს.

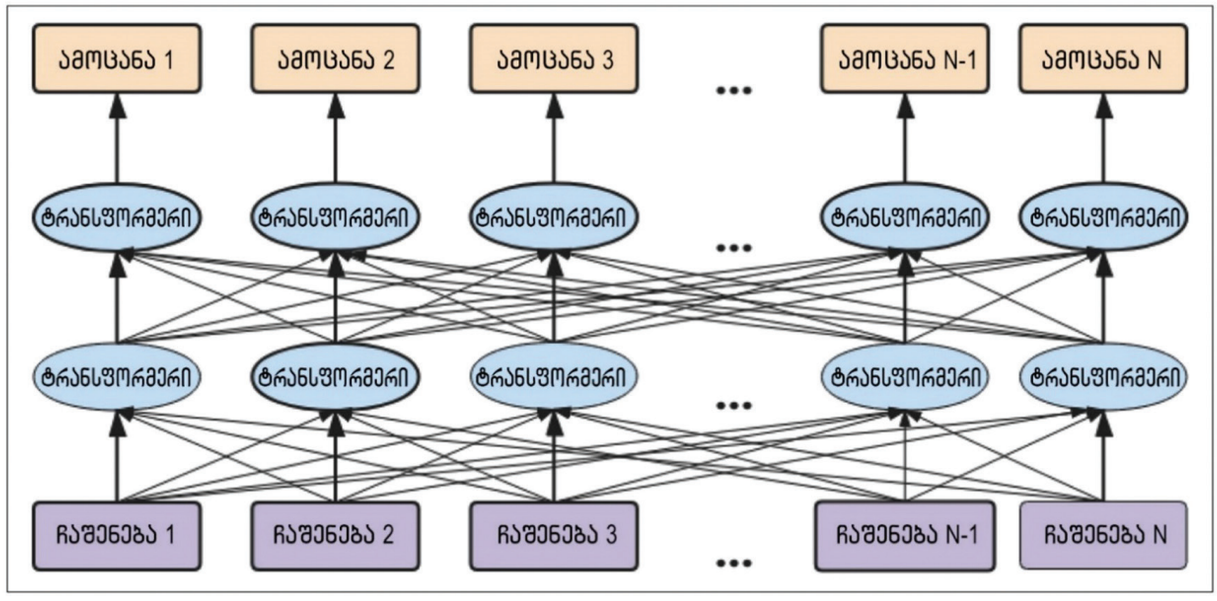
თავდასხმა და ქურდობა: თავდამსხმელები იყენებენ თავდასხმის მრავალ მეთოდს, როგორიცაა: შუბის, წყლის ხვრელის, DoS-ის, წყალდიდობის, ვინნუკის (WinNuke), მიწისზედა, სკრიპტ/აქტივ X-ის (Script/Active X), სმურფის (Smurf) და მარშრუტიზაციის პროტოკოლის თავდასხმები. მათ შეუძლიათ განახორციელონ შესაბამისი თავდასხმები სამიზნე მასპინძელზე ან მანქანაზე IIoT-ში და ეს მონაცემები ასევე შეიძლება ჩაიწეროს.

6.3.2. APT თავდასხმის სიტყვის ვექტორის გენერაცია

„სიტყვის ვექტორი“ არის სიტყვების ვექტორებად წარმოდგენა, ჩვეულებრივ, მრავალგანზომილებიანი უწყვეტი მცურავი მძიმით გამოსახული რიცხვების მიხედვით, სადაც მსგავსი სიტყვები გეომეტრიულ სივრცეში მსგავს ადგილებზეა განთავსებული. სიტყვების ვექტორებად წარმოდგენა მათემატიკურ ოპერაციებში მათი გამოყენების საშუალებას იძლევა. APT არის თავდასხმა, რომელიც შეუმჩნეველი რჩება დიდი ხნის განმავლობაში. შეგროვებული APT თავდასხმის მონაცემები IIoT-ში უნდა იყოს ვექტორიზებული, რათა გამოყენებულ იქნეს, როგორც შემავალი მონაცემები კლასიფიკაციის მოდელისთვის, რათა განასხვაოს თავდასხმის ტიპი. ქსელზე APT თავდასხმის მთელი პროცესის სხვადასხვა ეტაპზე, ქსელის მონაცემთა ყველა პაკეტი წარმოადგენს დროით მწკრივს. ვინაიდან შესაძლოა არსებობდეს გარკვეული კორელაცია ან ლოგიკური ურთიერთობა თავდასხმის ხუთ განზრახვას შორის, ყველა მათგანის ეტიკეტები გარდაიქმნება შესაბამის სიტყვით ვექტორებად. ტრადიციულ დისკრეტულ წარმოდგენას არ შეუძლია აჩვენოს ეს ურთიერთობა, ამიტომ განაწილებული წარმოდგენა გამოიყენება ამ სიტყვების განაწილებულ სიტყვის ვექტორის წარმოდგენაში გადასაყვანად. ამ განაწილებულ წარმოდგენას შეუძლია ასახოს ურთიერთკავშირი APT თავდასხმის განზრახვებს შორის IIoT-ში. ტრადიციულ ტექსტურ ინფორმაციაში, ყველაზე წარმომადგენლობითი სემანტიკური მახასიათებლების მქონე სიტყვები, როგორც წესი, შეირჩევა სიტყვის ვექტორის წარმოდგენისთვის. ეს ჩვეულებრივ კეთდება word2vec მოდელის გამოყენებით, რომელსაც შეუძლია თითოეული მახასიათებელი სიტყვა იმავე ფორმაში გარდაქმნას. თუმცა, როდესაც word2vec მოდელი გამოიყენება სიტყვის ვექტორის წარმოდგენისთვის, APT თავდასხმის მახასიათებლის სიტყვები არ შეიძლება გამოირჩეოდეს კონტექსტური სემანტიკური ინფორმაციის საშუალებით და თავდასხმის სხვადასხვა განზრახვა შეიძლება წარმოადგენდეს იმავე ვექტორს, რაც იწვევს კლასიფიკატორის შემდგომ არასწორ შეფასებებს. ამ მიზეზების გამო, ამ თავში გამოყენებულია ლიტერატურაში აღწერილი BERT მოდელი APT თავდასხმის განზრახვის სიტყვის ვექტორის წარმოსაჩენად. ჩვენ ვირჩევთ BERT-ს APT თავდასხმების მიმართ ხანგრძლივი მდგრადობის გამო. თუ თავდასხმის დროის ინტერვალი ძალიან დიდია, ძნელია თავდასხმების სრული ჯაჭვის აღმოჩენა რეალურ დროში, წერტილი-დროში (point-in-time) გამოვლენის ტექნოლოგიაზე დაყრდნობით. ამ თავში გამოყენებული BERT მოდელი შეიცავს ტრანსფორმერის სტრუქტურას, რომელიც ეყრდნობა ყურადღების მექანიზმს შემავალი და გამომავალი მონაცემების გლობალური დამოკიდებულების მოდელირებისთვის. მას შეუძლია აითვისოს APT თავდასხმების ძირითადი მახასიათებლები უცნობ დროით მწკრივებში. უფრო მეტიც, ამ მეთოდს შეუძლია დააკავშიროს კონტექსტი და სემანტიკური ინფორმაცია APT თავდასხმების მიმდევრობიდან და შეიძლება უფრო გონივრულად იყოს გამოხატული, როგორც განსჯის სიტყვის ვექტორი.

6.3.3. წინასწარი ტრენინგის BERT ენის მოდელი

როგორც ნახ. 6.2-ზეა ნაჩვენები, წინასწარი ტრენინგის BERT მოდელი იყენებს ორმხრივ ტრანსფორმერს, როგორც კოდერს; ეს ტრანსფორმერი დაფუძნებულია ტექსტის მოდელის ყურადღების მექანიზმზე, რომელსაც აქვს კარგი პარალელური გამოთვლითი შესაძლებლობები. თავდაპირველად, შემოთავაზებული იყო, რომ შენიღბული ენის მოდელი და წინადადების უწყვეტობის პროგნოზი გამოყენებული ყოფილიყო ერთობლივი ტრენინგისთვის. ზემოხსენებულ BERT მოდელს შეუძლია დააფიქსიროს ძირითადი მახასიათებლები უცნობ დროით მწკრივებში, რომელთაც აქვთ განსხვავებული სიგრძე IIoT-ზე APT თავდასხმისთვის. ჩვენ ვიყენებთ დამუშავებული APT თავდასხმების მიმდევრობის ჩაშენების გამომავალ მონაცემებს, როგორც BERT ტრანსფორმერის შიდა კოდირების ქსელის შემავალი მონაცემების სიტყვიერ წარმოდგენას, ტრანსფორმერის კოდერების მწკრივთან ერთად. BERT მოდელში, მრავალფენიანი ორმხრივი ტრანსფორმერის კოდერის გამოყენების შემდეგ, საბოლოოდ მიიღება APT თავდასხმის სიტყვის ვექტორირებული წარმოდგენის ამოცანები. ტრანსფორმერი არის Seq2Seq მოდელი, რომელიც დაფუძნებულია თვითყურადღებაზე, რომელსაც აქვს კოდერ-დეკოდერის სტრუქტურა. კოდერი ცვლადი სიგრძის მიმდევრობას ფიქსირებული სიგრძის მიმდევრობას ამატებს და დეკოდერი ახდენს ამ ფიქსირებული სიგრძის ვექტორის დეკოდირებას ცვლადი სიგრძის გამომავალ მიმდევრობაში. BERT მოდელი ძირითადად იყენებს ტრანსფორმერის კოდერის ნაწილს, რომელსაც შეუძლია APT თავდასხმაში ცვლადი სიგრძის დროითი მწკრივების კოდირება. კოდერის სტრუქტურა ნაჩვენებია ნახ. 6.3-ზე.



ნახ. 6.2. BERT მოდელის სტრუქტურა

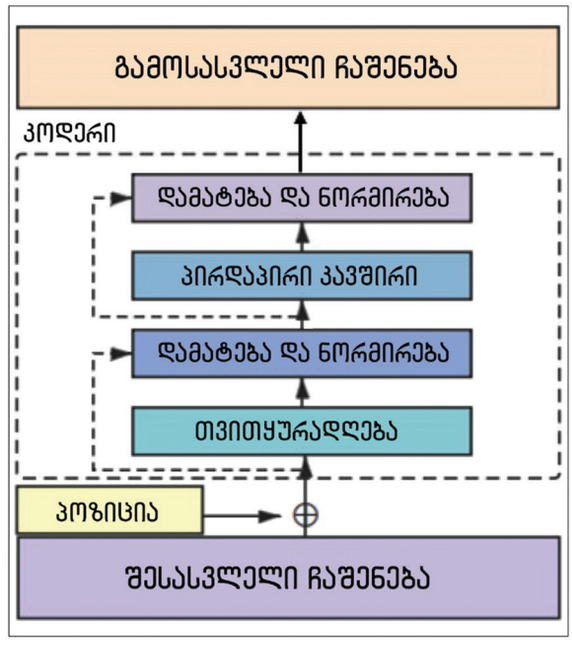
კოდერის შემავალი მონაცემები არის სიტყვის ჩაშენებული წარმოდგენა, სადაც ემატება პოზიციის შესახებ ინფორმაცია. შემავალი მონაცემები შემდეგ გადის თვითყურადღების ფენაში, რომელიც კოდერს ეხმარება დაათვალიეროს სიტყვების შესახებ ინფორმაცია თითოეული სიმბოლოს კოდირებამდე და მის შემდეგ. მისი გამომავალი მონაცემები გადის დამატებისა და ნორმირების ფენებს. დამატების ფენა ამატებს თვითყურადღების ფენის შემავალ და გამომავალ მონაცემებს, რასაც მოჰყვება ნორმალიზება ნორმირების ფენაში. ნორმალიზებული ვექტორების სია გადაეცემა პირდაპირი კავშირის ფენას, რომელიც სრულად დაკავშირებული ნეირონული ფენაა. პირდაპირი კავშირის ფენა მოჰყვება შესაბამის დამატების, ნორმირების ფენებს და მის გამოსასვლელზე ვიღებთ ნორმალიზებული სიტყვის ვექტორების ახალ სიას. კო-

დერში, თვითყურადღების გამოყენებით, ყველაზე მნიშვნელოვანი შემავალი მონაცემების განსაზღვრის ძირითადი იდეა არის მიმდევრობაში ტექსტური შეტყობინებისა და სხვა ტექსტური შეტყობინებების ურთიერთკავშირის გამოთვლა, შემდეგ კი ამ ურთიერთკავშირის გამოყენება თითოეული ტექსტის წონის დასარეგულირებლად და ახალი გამოხატვის მისაღებად. ეს ახალი გამოხატვა შეიცავს არა მხოლოდ მათ საკუთარ სემანტიკებს, არამედ მათ შორის ურთიერთობასაც. ამიტომ, ტრადიციულ სიტყვის ვექტორთან შედარებით, ის უფრო გლობალურ გამოხატვას იძლევა და IIoT-ის APT თავდასხმების მიმდევრობას შეუძლია უფრო გონივრულად გამოხატოს კონტექსტის სემანტიკური ინფორმაცია დროებით მახასიათებელში.

6.3.4. თავდასხმების მიმდევრობის ოპტიმიზაცია IIoT-ში

APT თავდასხმებში, თითოეულ თავდასხმას აქვს საფეხურები, თითოეულ საფეხურს აქვს საკვანძო სიტყვის ვექტორები და საფეხურებს შორის სიტყვის ვექტორები კორელაციაშია. ჩვენ ვიყენებთ ტერმინს „ვექტორული ასოციაციის ურთიერთობა“ თავდასხმების მიმდევრობის მონაცემების ოპტიმიზაციისთვის. APT თავდასხმების ზოგიერთი ოპერაცია, რომელიც არ აზიანებს მასპინძელს, შეიძლება ჩაითვალოს ჩვეულებრივ მონაცემად და არ ჩაითვლება APT თავდასხმების მიმდევრობის შაბლონებში. მხოლოდ სიტყვათა ვექტორული ასოციაციის ურთიერთობა ოპერაციების წინ და შემდეგ, რომლებიც აკმაყოფილებენ თავდასხმის მახასიათებლებს, გამოიყენება, როგორც APT-ის გამოვლენის მოდელის შემავალი მონაცემები. სხვა სიტყვებით რომ ვთქვათ, ჰაკერი ასრულებს გარკვეულ ოპერაციებს ზოგიერთ საფეხურზე, მაგრამ სანამ ეს მოქმედება არ ამოიღებს სიტყვის ვექტორს, რამაც შეიძლება ზიანი მოიტანოს, ჩვენ ამ ჰაკერულ ოპერაციას კვლავ ნორმალურ მონაცემად მივიჩნევთ, რომელიც არ იქნება გამოყენებული თავდასხმის ეტაპად. ამგვარად, ჩვენ თავიდან ავიცილებთ ყველა ოპერაციის თავდასხმად განხილვას (როგორც კი ისინი განიხილება ჰაკერებად) და ამით ვახდენთ თავდასხმის მიმდევრობის შაბლონების ოპტიმიზაციას.

ოპტიმიზაციის შემდეგ, APT თავდასხმების მიმდევრობის სიგრძე შეიძლება მნიშვნელოვნად შემცირდეს, რაც არა მხოლოდ უზრუნველყოფს APT თავდასხმების მიმდევრობის მახასიათებლების მთლიანობას, არამედ ამარტივებს APT თავდასხმების მიმდევრობას, რაც მნიშვნელოვნად ამცირებს მოდელის ტრენინგის ღირებულებას.



ნახ. 6.3. ტრანსფორმერის კოდერის სტრუქტურა

6.3.5. BERT-ზე დაფუძნებული APT თავდასხმის გამოვლენის ალგორითმი

განვიხილოთ APT თავდასხმის გამოვლენის ალგორითმი, რომელიც დაფუძნებულია BERT-ზე და გამოიყენება IIoT-ში. ალგორითმის პროცედურა შემდეგია:

შესასვლელი: ეს არის APT თავდასხმის თანმიმდევრობის ტრენინგი IIoT-ში, სადაც შედის ორი ცვლადი: ერთი არის APT თავდასხმის დამახასიათებელი ინფორმაცია, მეორე კი APT კატეგორია, რომელსაც მიეკუთვნება თავდასხმა.

გამოსასვლელი: ეს არის APT თავდასხმის განზრახვის კლასიფიკაციის მოდელი.

ნაბიჯი 1: პირველ ეტაპზე სუფთა მონაცემთა ნაკრები მიიღება შეგროვებული მონაცემების გაწმენდით და წინასწარი დამუშავებით. მონაცემთა გაწმენდისთვის, ჩვენ ძირითადად, ვშლით ნული (null) ატრიბუტის მნიშვნელობებს APT თავდასხმის შაბლონში. მონაცემთა წინასწარი დამუშავებისთვის, ვნომრავთ APT თავდასხმების სიმბოლოების ატრიბუტებს, ვასრულებთ ერთჯერად „ცხელ“ კოდირებას ატრიბუტის მრავალ მნიშვნელობაზე და ვაკავშირებთ შედეგს თავდაპირველ ატრიბუტთან. რიცხვითი და ერთჯერადი კოდირებით დამუშავების შემდეგ, რადგან თითოეული ატრიბუტის რიცხვითი დიაპაზონი განსხვავებულია, ორიგინალური მნიშვნელობის პირდაპირი გამოყენება გავლენას მოახდენს მოდელის ფოკუსის ცვლილებაზე, ამიტომ მონაცემთა ნაკრების მახასიათებლები სტანდარტიზებულია და ნორმალიზდება.

ნაბიჯი 2: წინასწარ დამუშავებული APT თავდასხმების მიმდევრობის მონაცემები იგზავნება BERT მოდელში, სადაც სინქრონიზაციის ფუნქცია იწყება [CLASS (CLS)]-ით, ხოლო ფუნქციისა და თეგის კატეგორია განცალკევებულია [SEPARATING (SEP)] აღნიშვნით.

ნაბიჯი 3: წინასწარი ტრენინგის BERT მოდელში მონაცემები კოდირებულია ორმხრივი ტრანსფორმერის კოდერით. ხორციელდება APT თავდასხმების მიმდევრობის შესაბამისი მახასიათებლების აღნიშვნა.

ნაბიჯი 4: მე-3 ნაბიჯზე მიღებული მახასიათებელი წარმოდგენა შეყვანილია Softmax რეგრესიის კლასიფიკატორის მოდელში კლასიფიკაციის ტრენინგისთვის, სადაც სიტყვის ვექტორის განზომილება დაყენებულია 5-ზე, რათა მივიღოთ ალბათობა იმისა, რომ APT თავდასხმის განზრახვა ეკუთვნის APT თავდასხმების თითოეულ მიმდევრობას.

ნაბიჯი 5: ტრენინგის ნაკრების მონაცემები დატრენინგდება ჯგუფურად და შედეგები გამოდის APT თავდასხმის განზრახვების კლასიფიკაციის მოდელზე.

ნაბიჯი 6: მიღებული კლასიფიკაციის მოდელი გამოიყენება სატესტო კომპლექტზე მოდელის განზოგადების უნარის შესამოწმებლად და ალგორითმის შესრულების სხვადასხვა ინდიკატორის მისაღებად.

6.4. ექსპერიმენტული ანალიზი

ექსპერიმენტი შესრულებული იყო TensorFlow ღრმა სწავლების სტრუქტურის გამოყენებით. ექსპერიმენტული აპარატურის გარემო არის კომპიუტერი Windows 10 ოპერაციული სისტემით და NVIDIA GTX 1080TI GPU-თი. აღებული იყო გარკვეული აღჭურვილობის მწარმოებლისგან შეგროვებული მონაცემები, როგორც ექსპერიმენტული სასწავლო და სატესტო მონაცემთა ნაკრებები და სიმულაციის პროცესში თავდასხმები დაყოფილი გახლდათ სხვადასხვა კატეგორიად.

განხილული (BERT) სქემის ეფექტიანობის შესაფასებლად, შედარების სქემების შემუშავებისას, ჩვენ ვირჩევთ ერთფენიან პერცეპტრონის (Perceptron) მოდელს, ერთფენიან გრძელ მოკლევადიანი მეხსიე-

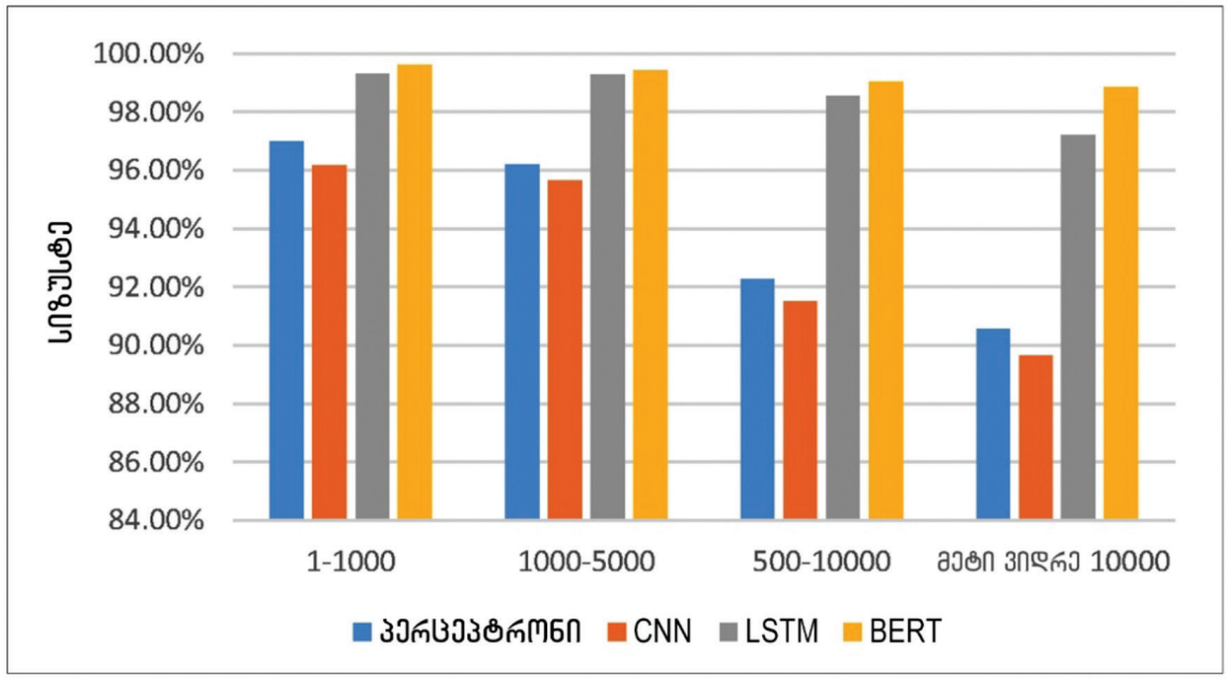
რების (LSTM) ქსელს და ერთფენიან კონვოლუციურ ნეირონულ ქსელს (CNN). ამ ქსელური მოდელის შერჩევის მიზეზი არის ის, რომ სასწავლო ნაკრები შედგება მხოლოდ 5-სიტყვიანი ვექტორებისგან; რადგან სიტყვის ვექტორების სიგრძე მცირეა, შესაბამისად, ნაკლები პარამეტრია საჭირო. პუნქტებად გაწერილი, დეტალური ექსპერიმენტული გეგმა ასეთია:

1. APT თავდასხმების მიმდევრობის გამოვლენის სიზუსტე: მონაცემები დაყოფილია ოთხ დონედ, მიმდევრობის სიგრძის მიხედვით, ანუ 1–1000, 1000–5000, 5000–10000 და 10000–ზე მეტი. ათჯერადი ჯვარედინი ვალიდაციის მეთოდი გამოიყენება APT თავდასხმების მიმდევრობის გამოვლენის სიზუსტის მაჩვენებლის მისაღებად.
2. მიმღების ოპერაციული მახასიათებლის (ROC) მრუდი: საფეხურები იგივეა, რაც პირველ პუნქტში. ოთხი დატრენინგებული მოდელი პროგნოზირებულია ტესტის კომპლექტზე და ROC მრუდები მიიღება მოდელის მუშაობის შედარებისთვის.

APT-ის გამოვლენის სიზუსტის მაჩვენებლები ოთხი მოდელისთვის ტესტის კომპლექტის მიმდევრობის სხვადასხვა სიგრძით ნაჩვენებია ცხრილში 6.1. ამ ცხრილიდან ჩვენ ასევე შეგვიძლია მივიღოთ APT-ის გამოვლენის სიზუსტის ჰისტოგრამა ოთხი მოდელისთვის, როგორც ნაჩვენებია ნახ. 6.4-ზე.

მიმდევრობის სიგრძე	პერცეპტრონი	CNN	LSTM	BERT
1–1000	97.00%	96.17%	99.31%	99.62%
1000–5000	96.20%	95.67%	99.26%	99.44%
5000–10000	92.26%	91.52%	98.56%	99.04%
10000–ზე მეტი	90.58%	89.66%	97.21%	98.85%

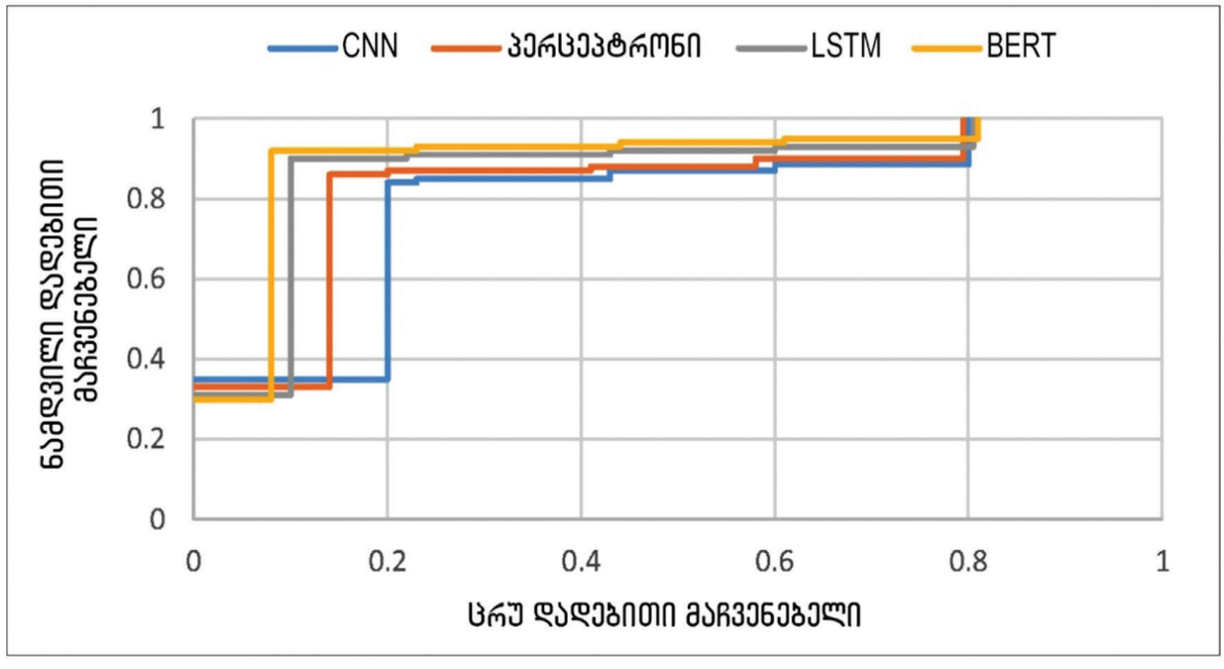
ცხრილი 6.1. მოდელებისთვის APT-ის გამოვლენის სიზუსტე მიმდევრობის სიგრძეების მიხედვით



ნახ. 6.4. მიმდევრობის მოდელების სიზუსტის პროცენტული კოეფიციენტების შედარების ჰისტოგრამა

ცხრილი 6.1-ისა და ნახ. 6.4-ის კომბინაცია ცხადყოფს, რომ როდესაც უცნობი თავდასხმების მიმდევრობა მოკლეა, მაგალითად, 1-დან 5000-მდე, ოთხივე მოდელს შეუძლია ამოიცნოს უცნობი APT თავდასხმები 95.67 პროცენტზე მეტი სწორი მაჩვენებლით; ეს წარმატება განპირობებულია მოკლე თავდასხმით. მიმდევრობის მახასიათებლები შეიძლება კარგად იქნეს ამოღებული ამ ოთხი მოდელის მიხედვით, განსხვავებების შესაფასებლად. მათ შორის, BERT მოდელს აქვს უმაღლესი სიზუსტე, რომელიც აღწევს 99.42 პროცენტზე მეტს, ხოლო LSTM იკავებს მეორე ადგილს, რაც მიუთითებს იმაზე, რომ ჩვენს მოდელს შეუძლია ეფექტიანად აღმოაჩინოს APT თავდასხმა, როდესაც შეყოვნება არ არის დიდი. თავდასხმების მიმდევრობის ხანგრძლივობის ზრდასთან ერთად, CNN და პერცეპტრონის მოდელები კარგავს ეფექტიანობას გრძელვადიანი შეყოვნების APT თავდასხმების გამოვლენისას. ეს იმიტომ ხდება, რომ ასეთ გრძელ უცნობ მიმდევრობებს არ შეუძლიათ ეფექტიანად ამოიღონ თავდასხმის მახასიათებლები ერთფენიანი ქსელის ან CNN სტრუქტურის გამოყენებით. LSTM და BERT მოდელებს შეუძლიათ კარგი შედეგების მიღება, რადგან მათ აქვთ მეხსიერება უფრო გრძელი მიმდევრობის მონაცემთა ფუნქციებისთვის; კერძოდ, BERT-ში შემავალი ტრანსფორმერის თვითყურადღებას შეუძლია სწორად შენიშნოს APT თავდასხმა, რაც მას საშუალებას აძლევს, საუკეთესო გამოვლენის ეფექტებს მიაღწიოს. ამგვარად, BERT მოდელს აქვს უკეთესი მახასიათებელი, ვიდრე სხვას. ჩვენ ვიყენებთ ოთხ დატრენინგებულ მოდელს სატესტო კომპლექტისთვის და ვიღებთ ROC მრუდებს, რომლებიც ნაჩვენებია ნახ. 6.5-ზე. ეს ნახაზი ნათლად აჩვენებს, რომ ROC მრუდების გადახრის ხარისხი 45°-იანი დიაგონალიდან თითქმის ერთნაირია ოთხივე მოდელისთვის. სიზუსტის ფართობი ROC მრუდის ქვეშ ოდნავ დიდია BERT მოდელისთვის, ვიდრე დანარჩენი სამისთვის. აქედან გამომდინარე, ვასკვნით, რომ ამ თავში აღწერილი მიდგომა უზრუნველყოფს უკეთეს მახასიათებლებს.

ერთად აღებული, პირველი და მეორე პუნქტების შესაბამისი შედარებითი ანალიზის შედეგები აჩვენებს, რომ ამ თავში მოცემულ მეთოდს შეუძლია კარგად აღმოაჩინოს APT თავდასხმების მიმდევრობა IIoT-ში თავდასხმის გრძელვადიანი ხანგრძლივობისას და აჩვენოს ამ მეთოდის მიზანშეწონილობა და ეფექტიანობა.



ნახ. 6.5. ROC მრუდების შედარების დიაგრამა

6.5. მეექვსე თავის დასკვნა

ცოტა ხნის წინ, 6G-ის როლი გამოიკვეთა IIoT დომენშიც. მაგალითად, ML მიდგომები გამოყენებული იქნა 6G-ზე დაფუძნებული IIoT ქსელების ინტელექტუალურობის უზრუნველსაყოფად. ლიტერატურაში შესწავლილია ML-ზე დაფუძნებული CNN-ების პოტენციალი რესურსების განაწილების ოპტიმიზაციის კუთხით მასობრივ IIoT სისტემებში 6G მრავალაგენტიანი სისტემის მეშვეობით. აღნიშნულიდან გამომდინარე, 6G ქსელების IIoT-ში APT-ის გამოვლენა თანდათან იქცა კვლევის ცხელ წერტილად, როგორც ინდუსტრიაში, ასევე აკადემიურ წრეებში და ახლახან გაჩნდა მრავალი ახალი ტექნოლოგია, ალგორითმი და სისტემა, რომლებიც დაკავშირებულია APT-ის გამოვლენასთან. იდუსტრიული მართვის სისტემების საგანგებო კიბერსიტუაციებზე რეაგირების ჯგუფის (ICS-CERT) მიერ ჩატარებული ინდუსტრიული ინტერნეტუსაფრთხოების სიტუაციის 2016 წლის ანგარიშის ანალიზის მიხედვით, ქვეყნის კრიტიკული ინფრასტრუქტურის 80 პროცენტზე მეტი ეყრდნობა ინდუსტრიულ ინტერნეტს, წარმოების პროცესის ავტომატიზაციისთვის.

თუმცა, APT-ის გამოვლენას არსებულ ინდუსტრიულ ინტერნეტში აქვს მრავალი ნაკლი, როგორიცაა სიზუსტის დაბალი მაჩვენებელი და ცრუ განგაშის მაღალი მაჩვენებელი. ეს თავი გვთავაზობს ღრმა სწავლებაზე დაფუძნებულ APT-ის გამოვლენის პროაქტიულ სქემას IIoT-სთვის. ექსპერიმენტული შედეგები აჩვენებს, რომ შემოთავაზებულ მეთოდს არა მხოლოდ აქვს მიზანშეწონილობა და ეფექტიანობა APT-ების გამოვლენაში, არამედ აღწევს სიზუსტის მაჩვენებელს 99 პროცენტამდე. ვიმედოვნებთ, რომ მომავალი კვლევები მოახდენს ამ მოდელის ოპტიმიზაციას და ამ ტექნოლოგიის 6G-ზე დაფუძნებულ IIoT-ში დანერგვას შეუწყობს ხელს.

თავი 7. ბლოკჩეინზე დაფუძნებული სანდო იდენტიფიკატორით მმართველობის სტრუქტურა საგნების ინდუსტრიული ინტერნეტისთვის

7.1. შესავალი

ბოლო რამდენიმე ათწლეულის განმავლობაში ინტერნეტი სწრაფად განვითარდა და არსებობს ტენდენცია, რომ სამომხმარებლო ინტერნეტი თანდათან გადავა წარმოებაზე ორიენტირებულ ინტერნეტზე. წარმოებაზე ორიენტირებული ინტერნეტის ერთ-ერთი ყველაზე მნიშვნელოვანი წარმომადგენელია IIoT, რომელიც ჩვენ წინა თავში განვიხილეთ. IIoT მხარდაჭერილი იქნება 5G/B5G/6G და სხვა საინფორმაციო და საკომუნიკაციო ტექნოლოგიებით ინტელექტუალურ მანქანებთან, ადამიანებთან და მასალებთან ერთად. პროდუქტიულობისა და ეკონომიკის უზარმაზარი გაუმჯობესების გამო, რომელიც შეიძლება IIoT-მა მოიტანოს, იგი გახდა გლობალური ტექნოლოგიების ინოვაციებისა და ინდუსტრიის კონკურენციის მთავარი მწვერვალი.

იდენტურობის გარჩევადობის ტექნოლოგია არის ინდუსტრიული გაციფრულების გასაღები და მონაცემთა მიმოქცევის საფუძველი IIoT-ში. ის უზრუნველყოფს კოდირების ერთიან სქემას, მონაცემთა სტანდარტულ სტრუქტურას, მონაცემთა მოპოვებისა და მართვის სრულ მეთოდებს. როგორც იდენტურობის გარჩევადობის ყველაზე ფართოდ გამოყენებული ტექნოლოგია, დომენის სახელების სისტემას (DNS) აქვს შეზღუდვები IIoT-ის საჭიროებების დასაკმაყოფილებლად, მისი გარჩევადობის არასაკმარისი განზომილების, ცენტრალიზაციისა და სუსტი უსაფრთხოების გამო. ზოგიერთი მკვლევარი ამ პრობლემების გადაჭრას პატჩების დადებით და სხვა მიდგომების გამოყენებით ცდილობდა. შემოთავაზებული იყო ნამეკოინი (Namecoin) DNS-ის დეცენტრალიზაციისა და მონაცემთა უსაფრთხოების უზრუნველყოფისთვის ბლოკჩეინის დახმარებით. შესწავლილი გახლდათ კონსორციუმ-DNS სწრაფი ალგორითმებით კონსორციუმის ბლოკჩეინის კონსენსუსის მისაღწევად. ასევე განხილული იყო დეცენტრალიზებული DNS ორდონიანი მოდელით. პერსპექტიულია ამ მიზნებით ჰენდლის (Handle) გამოყენებაც, რომელიც არის DNS-სგან დამოუკიდებელი, პრაქტიკაში გავრცელებული, იდენტურობის გარჩევადობის განაწილებული ტექნოლოგია მრავალგანზომილებიანი მონაცემებით. ჰენდლის იდეტიფიკატორი არის ნახევრად უნიკალური (უნიკალური გადატვირთვებს შორის) ნომერი, რომელიც განსაზღვრავს ყველა შემდგომ აუდიტირებულ მოვლენას, სანამ ობიექტი ღიაა.

თუმცა, ზემოაღნიშნული ტექნოლოგიები ჯერ კიდევ ვერ აკმაყოფილებენ IIoT-ის საჭიროებებს მტყუნების ერთი წერტილის, მონაცემთა გაყალბებისა და მმართველობის პროცესში გადახრების პრობლემების გადაჭრის კუთხით. IIoT-ის სცენარში განსაკუთრებით მნიშვნელოვანია ინდუსტრიული წარმოების უსაფრთხოებისა და მონაცემთა მიმოქცევის უზრუნველყოფა, ასევე მრავალი მხარის სამართლიანი უფლებები და სანდოობა. აუცილებელია იდენტურობის გარჩევადობის ახალი არქიტექტურის შემუშავება, რომელიც ბუნებრივად დაუჭერს მხარს იდენტურობის გარჩევადობის ტექნოლოგიას IIoT-ში და უზრუნველყოფს უკეთეს დეცენტრალიზაციასა და სანდოობას.

ამ თავში ჩვენ განვიხილავთ იდენტურობის გარჩევადობის გზას, სანდო იდენტიფიკატორით ერთობლივი მმართველობის არქიტექტურის (TICA) გამოყენებით, რომლისთვისაც პროტოტიპის სისტემა შექმნილი და დანერგილია. ძირითადი სამუშაო მოიცავს საიდენტიფიკაციო სერვისისთვის დეცენტრალიზებული სტრუქტურის შემუშავებას, იდენტიფიკატორის სასიცოცხლო ციკლის მართვას ჭკვიანი კონტრაქტის საფუძველზე და მონაცემთა შენახვის მექანიზმის შეთავაზებას სანდო იდენტიფიკატო-

რისთვის. განხილული არქიტექტურა წარმოგვიდგენს ბლოკჩეინის მახასიათებლებს ჰენდლზე დაფუძნებული იდენტურობის გარჩევადობის არქიტექტურის გასაუმჯობესებლად და მტყუნების ერთი წერტილის, მონაცემთა გაყალბებისა და მმართველობის პროცესში გადახრების პრობლემების გადასაჭრელად. გარდა ამისა, TICA-ის ზოგიერთმა იდეამ შეიძლება უზრუნველყოს საჭირო გადაწყვეტილებები და წარმოქმნას ახალი მიდგომები იდენტურობის გარჩევადობისა და IIoT-სთვის.

მეშვიდე თავის დანარჩენი ნაწილი ორგანიზებულია შემდეგნაირად: პირველ რიგში წარმოდგენილი იქნება ლიტერატურაში არსებული კვლევების მოკლე მიმოხილვა და შესაბამისი ტექნოლოგიები. ტექნიკური გამოწვევებისა და დიზაინის პრინციპების ანალიზის შემდეგ, ჩვენ განვიხილავთ TICA-ის და აღვწერთ მის სტრუქტურას, დეტალებს. შემდეგ წარმოდგენილი იქნება ექსპერიმენტის შედეგები და ანალიზი. ასევე განიხილება ღია საკითხები. დაბოლოს, მოვიყვანთ შესაბამის დასკვნებს და გამოვყოფთ სამომავლო სამუშაოებს.

7.2. დაკავშირებული კვლევითი სამუშაოები

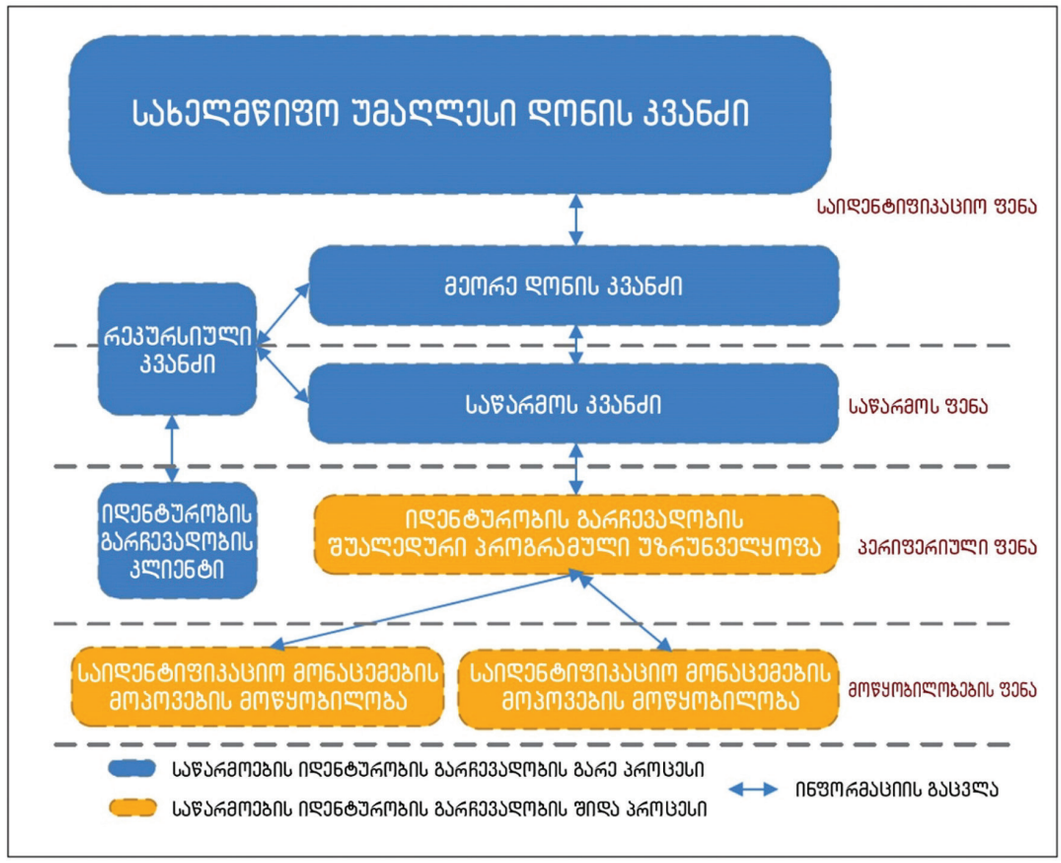
IIoT უზრუნველყოფს მანქანებსა და საინფორმაციო ქსელებს შორის ურთიერთკავშირს და ინოვაციურ გადაწყვეტილებებს სხვადასხვა ინდუსტრიისთვის საოპერაციო ხარჯების დაზოგვისა და სისტემის საიმედოობის გასაუმჯობესებლად. გაციფრულება არის ერთ-ერთი ყველაზე მნიშვნელოვანი პირობა IIoT-სთვის, რომ აჩვენოს თავისი პოტენციალი. აქტივების ადმინისტრირების გარსის (AAS) კონცეფცია ეხმარება IIoT-ს, უკეთ განახორციელოს გაციფრულების პროცესი.

AAS, ანუ აქტივების ვირტუალური წარმომადგენლობა უზრუნველყოფს ინტერფეისს მონაცემთა ურთიერთქმედების განსახორციელებლად. მას აქვს მრავალი სასარგებლო ფუნქცია, როგორიცაა: ინფორმაციის ინტეგრაცია, მონაცემთა კონტროლი, ორკესტრირება და ავტომატიზაცია. საიდენტიფიკაციო სერვისს შეუძლია დაეხმაროს AAS-ის აღნიშნული ფუნქციების განხორციელებაში. გარდა ამისა, საიდენტიფიკაციო სერვისის შექმნა შეიძლება გახდეს IIoT-ის პრიორიტეტი. მიზეზები შემდეგია:

1. საიდენტიფიკაციო სერვისი უზრუნველყოფს საიდენტიფიკაციო მონაცემების მოპოვების, იდენტიფიკატორის რეგისტრაციის, იდენტურობის გარჩევადობის, მონაცემთა დამუშავებისა და მოდელირების ფუნქციებს. ის მნიშვნელოვან როლს ასრულებს მონაცემთა სტანდარტიზებული ენკაფსულაციისა და ადრესაციის დროს.
2. საიდენტიფიკაციო სერვისის მიერ მოწოდებულ მონაცემთა განაწილებული ინტეგრაციის ფუნქციას შეუძლია უკეთ დაუჭიროს მხარი ზედა ფენის მდიდარ აპლიკაციურ ეკოლოგიას. ამრიგად, სამართლიან და უსაფრთხო საიდენტიფიკაციო სერვისს აქვს პოტენციალი, ფართოდ იქნეს გამოყენებული ინდუსტრიულ აპლიკაციებში, როგორიცაა: სასიცოცხლო ციკლის მართვა, პროდუქტის მიკვლევადობა და მიწოდების ჯაჭვის მართვა.

IIoT-ის სტაბილური განვითარებით, შემოთავაზებულია ინდუსტრიული ინტერნეტის იდენტურობის გარჩევადობის სისტემის სტრუქტურა, როგორც ნაჩვენებია ნახ. 7.1-ზე. სტრუქტურა ძირითადად შედგება: სახელმწიფო უმაღლესი დონის კვანძისგან, მეორე დონის კვანძისგან, საწარმოს კვანძისგან და რეკურსიული კვანძისგან. ეს კვანძები ქმნიან ფენოვან სტრუქტურას ზემოდან ქვემოთ. მეორე დონის კვანძები არის საჯარო, რომლებიც ინდუსტრიულ საწარმოებს აწვდიან მინიჭებულ იდენტიფიკატორს, იდენტიფიკატორის რეგისტრაციისა და იდენტურობის გარჩევადობის ფუნქციებს. რეკურსიული კვანძი არის ინდუსტიულ მონაცემთა რესურსების ძირითადი ელემენტი, რომელიც უნდა იყოს თავსებადი

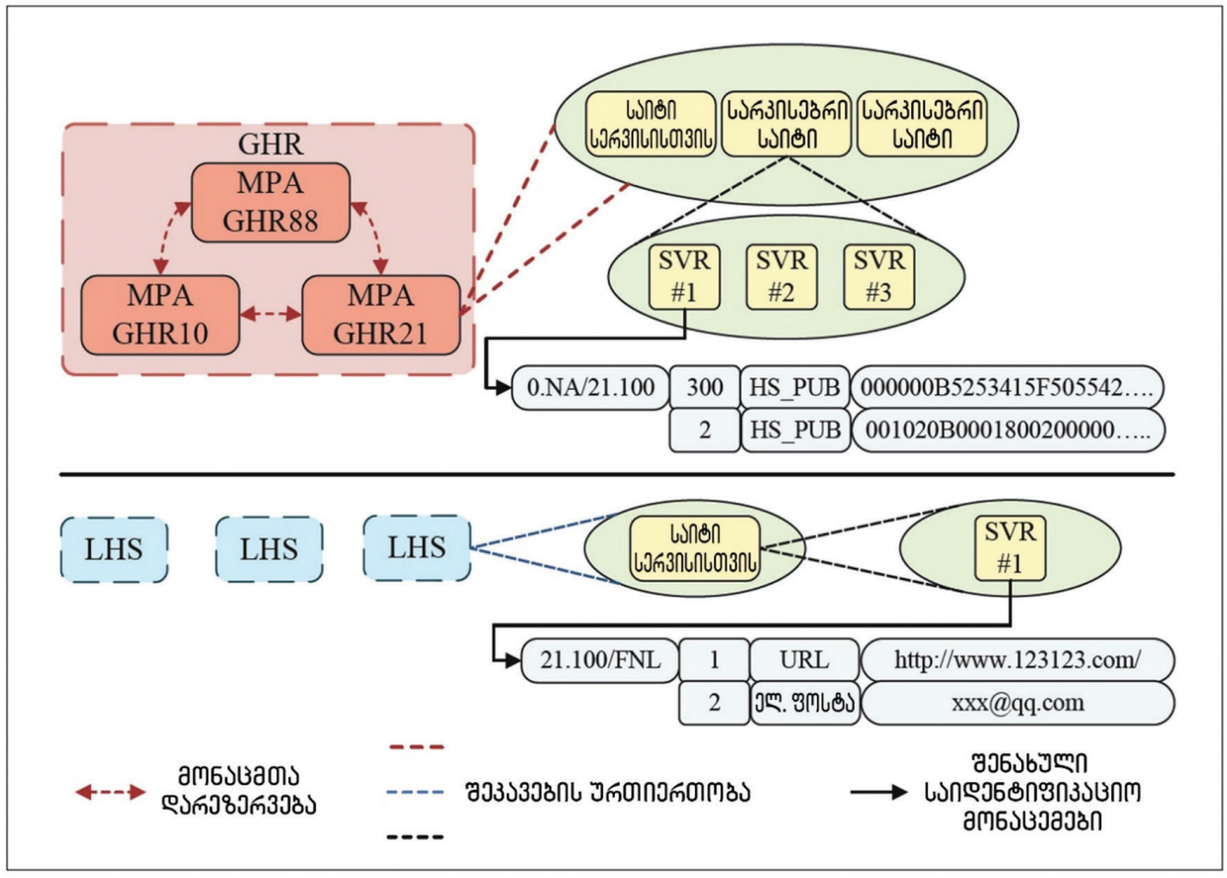
გარჩევადობის სხვადასხვა პროტოკოლთან, რათა დასრულდეს გარჩევადობის კუთხით დამუშავება და გააუმჯობესდეს მწარმოებლურობა ზოგიერთი ტექნოლოგიის საშუალებით (მაგალითად, ქეშირების ტექნოლოგიით).



ნახ. 7.1. ინდუსტრიული ინტერნეტის იდენტურობის გარჩევადობის სისტემის სტრუქტურა

სხვადასხვა ტექნოლოგიას (როგორიცაა მაგალითად, DNS) აქვს საკუთარი მახასიათებლები, მაგრამ ვერც ერთი მათგანი სრულად ვერ აკმაყოფილებს IIoT-ის მოთხოვნებს. ციფრული ობიექტების კონცეფციიდან გამომდინარე, ჰენდლი შეიძლება IIoT-სთვის სარგებელიანი იყოს. მას შეუძლია უკეთ ამოიცნოს, მართოს და მიიღოს ფიზიკური ობიექტების მრავალგანზომილებიანი მონაცემები. გარდა ამისა, ჰენდლს აქვს მოწყობილობისა და პლატფორმის დამოუკიდებლობის მახასიათებლები და შესაფერისია ჰეტეროგენული მონაცემების თავსებადობის პრობლემების გადასაჭრელად, დომენებს შორის ინფორმაციული ურთიერთქმედების სცენარებში.

ჰენდლის სისტემას აქვს ორფენიანი სერვისის სტრუქტურა, როგორც ნაჩვენებია ნახ. 7.2-ზე. ზედა ფენა არის ჰენდლის გლობალური რეგისტრი (GHR), ხოლო ქვედა – ჰენდლის ლოკალური სერვისი (LHS). ორივე GHR და LHS შედგება მრავალი საიტისგან. საიტები უზრუნველყოფენ სპეციალურ სერვისებს GHR-ისა და LHS-სთვის და მონაცემთა სინქრონიზაცია მიიღწევა სხვადასხვა საიტს შორის, რომლებიც უზრუნველყოფენ ერთსა და იმავე სერვისს. სერვერი არის საიტის ფიზიკური შემსრულებელი. ერთი ან რამდენიმე სერვერი ერთობლივად ინახავს მონაცემებს საიტის მიერ მოწოდებული საიდენტიფიკაციო სერვისის კონკრეტული ფუნქციების განსახორციელებლად, როგორიცაა: ჩაწერა, განახლება, წაშლა და მოთხოვნა. ზოგჯერ, გარკვეული სცენარებისთვის მონაცემთა მართვის საჭიროებების დასაკმაყოფილებლად, როგორიცაა პროდუქტის მონიტორინგი IIoT-ში, ჰენდლმა შეიძლება გამოიყენოს მრავალდონიანი LHS.



ნახ. 7.2. ჰენდლის სისტემის სერვისის სტრუქტურა (აკრონიმები მოცემულია წიგნის ბოლოს, განყოფილებაში: აბრევიატურები და აკრონიმები)

ჰენდლის იდენტიფიკატორი შედგება ორი ნაწილისაგან: პრეფიქსი და სუფიქსი. ჰენდლის სისტემაში ძირითადად, ორი ტიპის მონაცემებია, რომლებიც შემდეგნაირად არის განსაზღვრული:

უფლებამოსილების ჰენდლი: მონაცემები, რომლებიც გამოიყენება ჰენდლის სერვისის სტრუქტურის მართვის ურთიერთობის დასადგენად;

საერთო ჰენდლი: მონაცემები, რომლებიც გამოიყენება აპლიკაციებისთვის ციფრული ობიექტების იდენტიფიცირებისა და შენახვის მიზნით.

პრეფიქსი იმართება GHR-ის მიერ და გლობალურად უნიკალურია. GHR ინახავს პრეფიქსის მფლობელის საიდენტიფიკაციო ინფორმაციას, ხოლო LHS წვდება IP მისამართს უფლებამოსილების ჰენდლის შექმნით. სუფიქსი იმართება LHS-ის მიერ და ადგილობრივად უნიკალურია. LHS უზრუნველყოფს გარჩევადობის სერვისებს ადგილობრივი ჰენდლის იდენტიფიკატორებისთვის საერთო ჰენდლის ფორმირებით და ქმნის უფლებამოსილების ჰენდლს დაქვემდებარებული პრეფიქსების სამართავად, რომელსაც შეუძლია ჰენდლის მართვა მრავალი პრეფიქსით, მაგრამ იგივე პრეფიქსის მქონე ჰენდლის მართვა შესაძლებელია მხოლოდ ფიქსირებული LHS-ის მიერ.

ბლოკჩეინი ზოგადად განიხილება, როგორც განაწილებული ლეჯერის ტექნოლოგია, რომელიც ვითარდება სრულფასოვანი შენახვის სისტემად და რომელიც, თავის მხრივ, დაფუძნებულია ლოგიკური კონტროლის ფუნქციებზე, როგორიცაა ჭკვიანი კონტრაქტები. ლიტერატურაში ფართოდაა წარმოდგენილი ბლოკჩეინის ზოგადი იერარქიული ტექნიკური სტრუქტურა და შეჯამებულია მისი მახასიათებლები, როგორიცაა: დეცენტრალიზაცია, გაყალბებისგან დაცვა, ღიაობა, გამჭვირვალობა და კონტრაქტის ავტონომია. ამ მახასიათებლების საფუძველზე, ზოგიერთმა მკვლევარმა განახორციელა IIoT-

ისა და ბლოკჩეინის ინტეგრაცია. მაგალითად, შემოთავაზებულია ანონიმური რეპუტაციის სისტემა, რომელიც დაფუძნებულია ბლოკჩეინზე, რათა გაუმჯობესებულიყო IIoT-ით ჩართული საცალო მარკეტინგის სანდოობა მომხმარებლის კონფიდენციალურობის შენარჩუნებით. ასევე შემოთავაზებულია არქიტექტურა, რომელიც აერთიანებს ბლოკჩეინს და პერიფერიულ გამოთვლებს IIoT-ში კრიტიკული ინფრასტრუქტურის უსაფრთხოებისა და მასშტაბურობის უზრუნველსაყოფად. შესწავლილია ბლოკჩეინზე დაფუძნებული იდენტიფიკატორის მართვის პროტოკოლი და კრედიტის მართვის სტრუქტურა მესამე მხარეებზე ზედმეტად დამოკიდებულების პრობლემის გადასაჭრელად. ასევე, რამდენიმე სამუშაო ეძღვნება მასშტაბურობის პრობლემის გადაჭრას და კვანტური რეზისტენტული ბლოკჩეინის დანერგვას IIoT სფეროში.

7.3. სანდო იდენტიფიკატორით ერთობლივი მმართველობის არქიტექტურა

იდენტურობის გარჩევადობის სისტემაში არსებული ზოგიერთი პრობლემის გადასაჭრელად, ეს თავი გვთავაზობს TICA არქიტექტურას. დიზაინის მთავარი მიზანია ბლოკჩეინისა და ჰენდლის ტექნოლოგიის სიღრმისეულად გაერთიანება. ის არა მხოლოდ აკმაყოფილებს ობიექტის იდენტიფიკატორისა და მონაცემთა შეგროვების საჭიროებებს, არამედ აუმჯობესებს მონაცემთა უსაფრთხოებას და მართვის სამართლიანობას იდენტურობის გარჩევადობის არქიტექტურაში.

ამ მოსაზრებებიდან გამომდინარე, IIoT-ის იდენტურობის გარჩევადობის არქიტექტურა უნდა შეესაბამებოდეს დიზაინის შემდეგ პრინციპებს:

უწყვეტი სერვისი: რაც შეეხება მტყუნების ერთ წერტილს, IIoT-ის იდენტურობის გარჩევადობის არქიტექტურამ უნდა უზრუნველყოს სერვისების სტაბილურობა და ხელმისაწვდომობა ღია გარემოში, რათა თავიდან აიცილოს მავნე თავდასხმები, როგორიცაა მაგალითად, DDoS, რომელიც იწვევს იდენტიფიკატორის რეგისტრაციის და გარჩევადობის შეფერხებას.

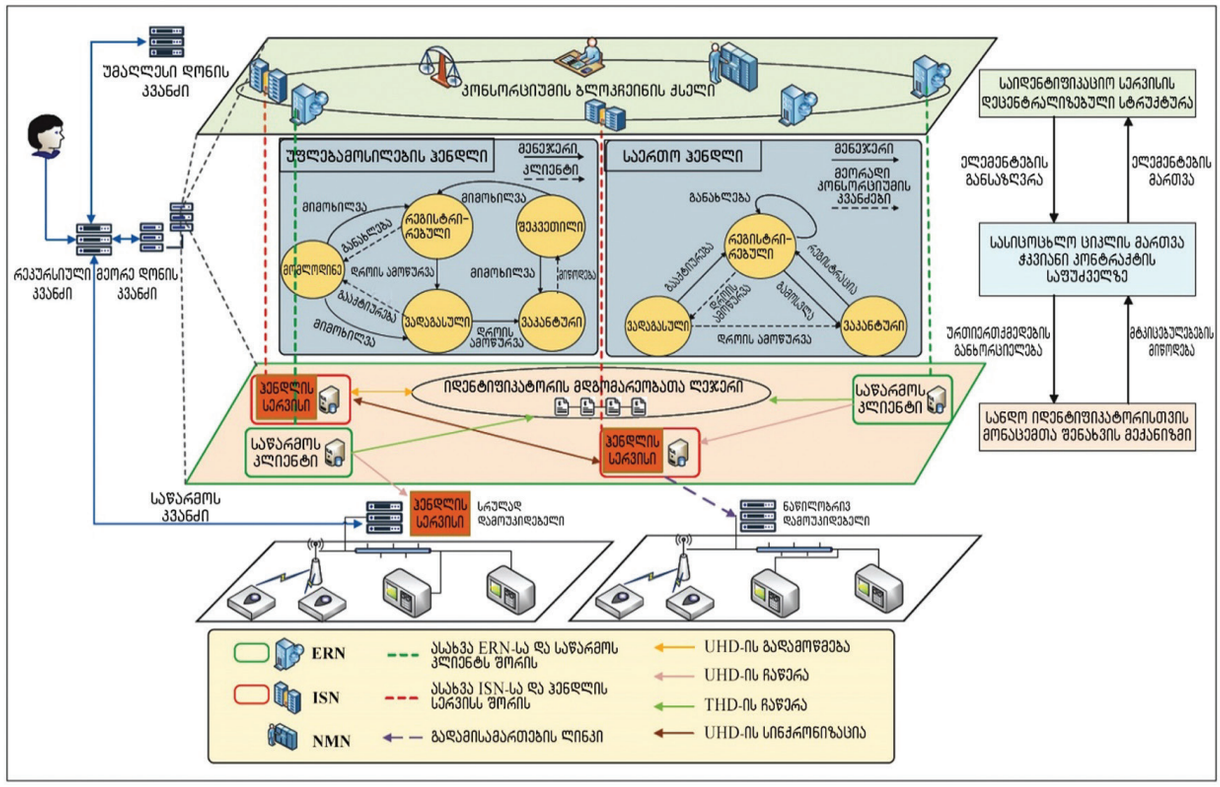
სანდო მონაცემები: რაც შეეხება მონაცემთა გაყალბებას, IIoT-ის იდენტურობის გარჩევადობის არქიტექტურას უნდა ჰქონდეს მონაცემთა მთლიანობის გადამოწმების და ქცევის მიკვლევადობის შესაძლებლობები. ეს თავიდან აგვაცილებს პასიური ხელყოფის მავნე ზემოქმედებას, ხელს შეუშლის საწარმოებში მონაცემთა აქტიურ ხელყოფას და შეამცირებს მონაცემთა ურთიერთდაკავშირების სანდოობის ღირებულებას.

დეცენტრალიზაცია: რაც შეეხება მმართველობის პროცესში გადახრას, მენეჯმენტის ქცევა IIoT-ის იდენტურობის გარჩევადობის არქიტექტურაში უნდა იყოს ღია და გამჭვირვალე, რაც გაზრდის საწარმოს კვანძების სანდოობას მეორე დონის კვანძებში და გააუმჯობესებს მონდომებას საწარმოს წვდომისთვის.

ზემოაღნიშნული დიზაინის პრინციპების გათვალისწინებით, ჩვენ განვიხილავთ TICA-ის. ჰენდლზე დაფუძნებული TICA იყენებს მრავალდონიან LHS სტრუქტურას და იყოფა სამ დონედ: პირველი დონე არის უმაღლესი დონის კვანძი, რომელიც მხარდაჭერილია ზოგიერთი ქვეყნის მიერ და პასუხისმგებელია მეორე დონის მართვაზე; მეორე დონეს შემოაქვს ბლოკჩეინი და აფართოებს მეორე დონის კვანძს მეორე დონის კონსორციუმის ბლოკჩეინის ქსელამდე, რომელიც აკავშირებს დონის კვანძსა და საწარმოს კვანძს. მას ემსახურება სხვადასხვა კომპანია და ორგანიზაცია. მეორე დონე უზრუნველყოფს კონკრეტული ინდუსტრიებისთვის ან მრავალი ინდუსტრიისთვის იდენტურობის გარჩევადობის ეფექტურ და სტაბილურ სერვისს; მესამე დონე არის საწარმოს კვანძი, რომელსაც შიგნიდან

მხარს უჭერს საწარმო და სერვისები. ის არა მხოლოდ იცავს საწარმოების მონაცემთა კონფიდენციალურობას, არამედ საშუალებას აძლევს საწარმოებს, IIoT მონაცემთა რესურსების აუზს დაუკავშირდნენ. გარდა ამისა, საწარმოს კვანძის განლაგების ტიპი შეიძლება დაიყოს სამ სახეობად, რომლებიც არის სრულად დამოუკიდებელი, ნაწილობრივ დამოუკიდებელი და სრულად მეურვეობის ქვეშ. საწარმოს იდენტურობის გარჩევადობის სერვისი სულ უფრო მეტად ხდება დამოკიდებული მეორე დონის კვანძზე.

TICA-ის მეორე დონის კვანძი შედგება სამი ნაწილისგან, რომლებიც არის საიდენტიფიკაციო სერვისის დეცენტრალიზებული სტრუქტურა, იდენტიფიკატორის სასიცოცხლო ციკლის მართვა ჭკვიანი კონტრაქტის საფუძველზე და სანდო იდენტიფიკატორისთვის მონაცემთა შენახვის მექანიზმი. სამი ნაწილი ნაჩვენებია ნახ. 7.3-ზე მარჯვნივ და ზოგიერთი დეტალი ჩანს ნახ. 7.3-ზე – მარცხნივ.



ნახ. 7.3. *სანდო იდენტიფიკატორით ერთობლივი მმართველობის არქიტექტურა*

საიდენტიფიკაციო სერვისის დეცენტრალიზებული სტრუქტურა ორიენტირებულია IIoT-ის მეორე დონის კვანძის სცენარებზე, ჰენდლის ეფექტიანი, ფენებად დაყოფილი სერვისის არქიტექტურის უპირატესობებზე დაყრდნობით და ბლოკჩეინის დეცენტრალიზებული სამუშაო მექანიზმის ჩართვით. იგი განსაზღვრავს მრავალ როლს და აყალიბებს მათ მენეჯმენტურ ურთიერთობებს, რაც აუმჯობესებს LHS-ის მრავალდონიან სტრუქტურას. იდენტიფიკატორის სასიცოცხლო ციკლის მართვის მეთოდი განსაზღვრავს უფლებამოსილების ჰენდლის და საერთო ჰენდლის მდგომარეობებიდან ურთიერთგადასვლის წესებს. ის აყალიბებს ჰენდლის სერვისის გარჩევადობის მექანიზმს და მართვის მექანიზმს ჭკვიანი კონტრაქტის საფუძველზე. სანდო შენახვის მექანიზმი აერთიანებს ჰენდლის განაწილებული შენახვის მეთოდს და ბლოკჩეინის განაწილებული ლეჯერის ტექნოლოგიას, რათა შეიმუშაოს იდენტიფიკატორის მდგომარეობათა ლეჯერი, შენახვისა და სინქრონიზაციის კლასიფიცირებული მეთოდები.

7.4. სანდო იდენტიფიკატორით ერთობლივი მმართველობის არქიტექტურის განხორციელების მეთოდები

ზემოაღნიშნული დიზაინის იდეებიდან და სტრუქტურის საერთო აღწერილობიდან გამომდინარე, ქვემოთ წარმოვადგენთ განხორციელების კონკრეტულ დეტალებს.

კონსორციუმის ბლოკჩეინის ქსელი შედგება მეორე დონის კონსორციუმის კვანძისგან. მისი სანდოობის ფუნდამენტი აგებულია მონაწილეთა მიერ მთელი ინდუსტრიიდან/რეგიონებიდან, ამიტომ იგი აჩვენებს დეცენტრალიზაციის მახასიათებლებს. მეორე დონის კონსორციუმის კვანძში არის სამი ტიპის კვანძი: ქსელის მართვის (NMN), საიდენტიფიკაციო სერვისის (ISN) და საწარმოთა რეგისტრაციის კვანძი (ERN). ბლოკის გენერირების, კონსენსუსის და ლეჯერის მომსახურების პროცესები სრულდება დანიშნული წევრების მიერ.

NMN პასუხისმგებელია ქსელის მშენებლობაზე, ქსელის და თითოეული კვანძის სტატუსის მონიტორინგზე. ის ასევე არის გადაწყვეტილების ცენტრი კონსორციუმის ბლოკჩეინის კონსენსუსის ალგორითმის შერჩევისთვის.

ISN პასუხისმგებელია საწარმოს პრეფიქსის გამოყოფაზე (მაგალითად, 88.100.1) და საწარმოს პრეფიქსის უფლებამოსილების ჰენდლის მართვაზე. ის ასევე უზრუნველყოფს იდენტურობის გარჩევადობის გარე სერვისს და საჯარო სერვისს, როგორიცაა იდენტიფიკატორის მუშაობისა და მიკვლევადობის მიმოხილვა. ISN-ებს შორის საიდენტიფიკაციო მონაცემები თანმიმდევრულია. გარდა ამისა, ISN-ის შეუძლია საწარმოებს მიაწოდოს მონაცემთა შენახვის სრულად მართული სერვისები.

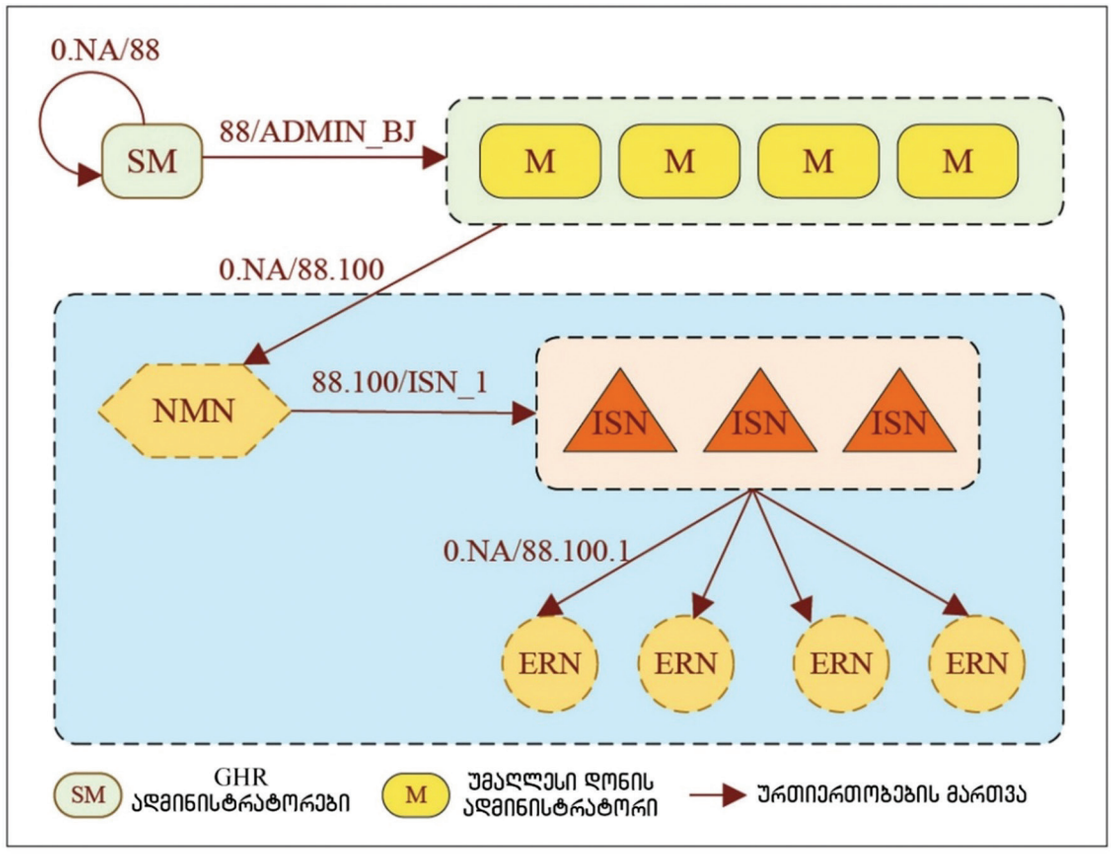
ERN ახდენს მონაცემთა მართვის სხვადასხვა ოპერაციის ინიცირებას საერთო ჰენდლებისთვის საწარმოს პრეფიქსის მიხედვით (მაგალითად, 88.100.1/მაგალითი) და ზედამხედველობას უწევს საწარმოს უფლებამოსილების ჰენდლის სასიცოცხლო ციკლს (მაგალითად, 0.NA/88.100.1). გარდა ამისა, მას შეუძლია მონაწილეობა სანდო შენახვაში და კონკრეტული მონაცემების მთლიანობის გადამოწმებაში საკუთარი საჭიროებების შესაბამისად.

საიდენტიფიკაციო სერვისისთვის დეცენტრალიზებული გარემოს სამუშაო პროცესი ნაჩვენებია ნახ. 7.4-ზე. სტრუქტურაში არის ხუთი როლი: GHR ადმინისტრატორი, უმაღლესი დონის კვანძის ადმინისტრატორი, NMN, ISN და ERN. ყველა როლს შორის ურთიერთობა ჩამოყალიბებულია ჰენდლის მრავალდონიანი სტრუქტურით.

NMN არის მეორე დონის პრეფიქსის მფლობელი და მართავს კონსორციუმის ბლოკჩეინის ქსელს. მას შეუძლია შექმნას იდენტიფიკატორები მეორე დონის პრეფიქსის ქვეშ, მაგრამ არ შეუძლია საწარმოს პრეფიქსის მინიჭება და საწარმოს იდენტიფიკატორის გადამოწმება. NMN-ის მიერ შექმნილი ISN უზრუნველყოფს საწარმოებისთვის პრეფიქსის განაწილებისა და იდენტურობის გარჩევადობის სერვისებს, ამიტომ ის არის საწარმოების საიდენტიფიკაციო სერვისის პროვაიდერი. ERN პასუხისმგებელია საერთო ჰენდლის მართვაზე საწარმოს პრეფიქსის მიხედვით. მისი ფუნქციონირების დაწყებამდე საჭიროა ISN-ის მიერ ავთენტიფიკაცია. მეორე დონის კონსორციუმის ბლოკჩეინის ქსელში მართვის პროცესს ასრულებენ მონაწილე კვანძები, რომლებიც იცავენ ჭკვიანი კონტრაქტით განსაზღვრულ წესებს. ცვლილებებისა და სტატუსის მონაცემები ჩაიწერება ლეჯერში და კონტროლდება ყველა კვანძით.

დომენის სახელების გარჩევადობის სისტემები (როგორიცაა Namecoin და Blockstack), რომლებიც მთლიანად დაფუძნებულია ბლოკჩეინზე, ახორციელებენ ავტონომიას ჭკვიანი კონტრაქტების ან სკრიპტირების ენების გამოყენებით. იდენტიფიკატორის სასიცოცხლო ციკლის მენეჯმენტი გულისხმობს ინფორმაციისა და პროცესების მართვას ჰენდლის საიდენტიფიკაციო მონაცემების სასიცოცხლო ციკლში პრეფიქსის აპლიკაციიდან და ასევე, პრეფიქსის შექმნის, განახლების, გაუქმებისა და ვა-

დის ამოწურვის მონაცემებიდან, გარდამავალი მდგომარეობის წესების შედგენით. საიდენტიფიკაციო სერვისის სტრუქტურაში, რომელიც დაფუძნებულია დეცენტრალიზებულ LHS სტრუქტურაზე, NMN, ISN და ERN ახორციელებენ უფლებამოსილების ჰენდლისა და საერთო ჰენდლის კოორდინირებულ ერთობლივ მმართველობას იდენტიფიკატორის სასიცოცხლო ციკლის მართვის მეთოდით. მეორე დონის კონსორციუმის კვანძი ზედამხედველობას უწევს შესაბამისი ჰენდლის მდგომარეობის ცვლილებას ჭკვიანი კონტრაქტის მეშვეობით. ის არა მხოლოდ უზრუნველყოფს ზედამხედველობის ეფექტურ საშუალებებს, არამედ ამცირებს ცენტრალიზაციის ხარისხს და მმართველობის პროცესში გადახრებს თავიდან აიცილებს.



ნახ. 7.4. საიდენტიფიკაციო სერვისის დეცენტრალიზებული სტრუქტურა

სხვადასხვა იდენტიფიკატორის სასიცოცხლო ციკლი იმართება სხვადასხვა როლით. როლები ძირითადად იყოფა: მენეჯერად, კლიენტად და ხელმძღვანელად. მენეჯერი პასუხისმგებელია ჰენდლის შინაარსის შეცვლაზე. იგი გათვალისწინებულია NMN-ის, ISN-ის ან ERN-ის მიერ. კლიენტს შეუძლია წარმოადგინოს შექმნის ან განახლების მოთხოვნა. ეს გათვალისწინებულია ISN-ის ან ERN-ის მიერ. ზედამხედველი პასუხისმგებელია მთელი პროცესის ზედამხედველობაზე, რომელიც შეესაბამება წინასწარ დადგენილ წესებს მმართველობითი გადახრების თავიდან ასაცილებლად. იგი გათვალისწინებულია მეორე დონის კონსორციუმის კვანძის მიერ.

იდენტიფიკატორის მდგომარეობის მართვა არის იდენტიფიკატორის სასიცოცხლო ციკლის მართვის გასაღები. მენეჯერს და კლიენტს აქვთ საკუთარი ოპერაციების ნაკრები. ეს ოპერაციები ჩაიწერება ბლოკში, მაგრამ მდგომარეობის გენერირებული ცვლილების შედეგები ჩაიწერება იდენტიფიკატორის მდგომარეობათა ლეჯერში. უფლებამოსილების ჰენდლის და საერთო ჰენდლის მდგომარეობებს შორის გადასვლის წესები განისაზღვრება შემდეგნაირად:

უფლებამოსილების ჰენდლი: ნახ. 7.3 გვიჩვენებს უფლებამოსილების ჰენდლის მდგომარეობებიდან გადასვლის წესებს. მას ძირითადად აქვს ხუთი მდგომარეობა: ვაკანტური, შეკვეთილი, რეგისტრირებული, ვადაგასული და მომლოდინე. თუ ორგანიზაციას სურს გახდეს საიდენტიფიკაციო სერვისის კვანძი მეორე დონის კონსორციუმის კვანძში, ორგანიზაციამ ჯერ უნდა შეიტანოს განაცხადი უფლებამოსილების ჰენდლის ადმინისტრატორის შესაქმნელად და წარადგინოს საიტის საჯარო გასაღები, საიტის ინფორმაცია და ა. შ. შექმნის პროცესი დასრულებულია ქსელის ადმინისტრატორის მიერ განხილვის შემდეგ. სანამ ადმინისტრატორის მოქმედების დრო ამოიწურება, საიდენტიფიკაციო სერვისის კვანძს შეუძლია შეიტანოს განაცხადი მონაცემთა მოდიფიკაციის შესახებ და მოდიფიკაცია დასრულდება ქსელის ადმინისტრატორის მიერ დადასტურების შემდეგ. მეორე დონის კონსორციუმის კვანძი განსაზღვრავს ჰენდლის გამოყენების პერიოდს ჭკვიანი კონტრაქტის საშუალებით. გამოყენების პერიოდის ამოწურვის შემდეგ, ადმინისტრატორს შეუძლია აიძულოს ჰენდლი შევიდეს ვადაგასულ მდგომარეობაში. თუ გარკვეული პერიოდის განმავლობაში აქტივაციის განაცხადი არ იქნება წარდგენილი, ჰენდლი გაუქმდება და შესაძლებელია მისი ხელახლა გამოყენება. ანალოგიურად, საწარმოს პრეფიქსის უფლებამოსილების ჰენდლმა ასევე უნდა გაიაროს მართვის ანალოგიური პროცესი.

საერთო ჰენდლი: საერთო ჰენდლს ძირითადად, აქვს სამი მდგომარეობა: ვაკანტური, რეგისტრირებული და ვადაგასული. ნახ. 7.3 გვიჩვენებს საერთო ჰენდლის მდგომარეობებიდან გადასვლის წესებს. საწარმოებს შეუძლიათ შექმნან იდენტიფიკატორები და თავად განაახლონ მონაცემები. მრავალორგანიზაციული მონაცემების გაზიარების სცენარში, კომპანიებს შეუძლიათ შექმნან გაზიარების კონტრაქტი გარკვეული იდენტიფიკატორებისთვის. როდესაც ვადის ამოწურვის განსაზღვრა შეუძლებელია, ეს ფუნქცია დაკავშირებულია კონკრეტულ აპლიკაციებთან და დეტალურად არ არის განხილული ამ თავში.

ციფრული აქტივების პროცესის შესახებ ინფორმაცია აღირიცხება განაწილებულ ლეჯერში. ბლოკჩეინი იყენებს „ბლოკს“ და „ჯაჭვს“ მონაცემთა სტრუქტურის ძირითადი მახასიათებლების აღსაწერად მის განაწილებულ ლეჯერში. IIoT-ის იდენტურობის გარჩევადობის სისტემაში იდენტიფიკატორის მდგომარეობათა მონაცემების შესანახად გამოიყენება ანგარიშზე დაფუძნებული მეთოდი. იდენტიფიკატორის მდგომარეობათა ლეჯერი აწარმოებს ჰენდლის მდგომარეობის შესახებ ინფორმაციის ჩაწერას.

საერთო ჰენდლის შენახვის მექანიზმი: მიუხედავად იმისა, რომ ბლოკჩეინს შეუძლია ეფექტიანად აიცილოს თავიდან გაყალბება და ასევე, მტყუნების ცალკეული წერტილები არ დაუშვას, არსებობს რესურსებზე დიდი ოვერჰედის პრობლემა. თუ ყველა იდენტიფიკატორი ინახება იდენტიფიკატორის მდგომარეობათა ლეჯერში, კვანძი ვერ შეძლებს დიდი რაოდენობის საიდენტიფიკაციო მონაცემების გატარებას. ამრიგად, მექანიზმი ახარისხებს ჰენდლის მონაცემებს ჰენდლის სანდო (THD) და არასანდო მონაცემებად (UHD). რესურსებზე ოვერჰედის გაზრდის და დაბალი ეფექტიანობის თავიდან აცილების მიზნით, სანდო მონაცემები ინახება იდენტიფიკატორის მდგომარეობათა ლეჯერში, როგორც ციფრული აქტივი, ხოლო არასანდო მონაცემები ინახება საიდენტიფიკაციო სერვისის კვანძის DB-ში.

THD მდგომარეობათა ლეჯერის სტრუქტურაში ჰენდლის იდენტიფიკატორი არის გასაღები, ხოლო მნიშვნელობების ნაკრები მოიცავს THD მონაცემებს, UHD გადამოწმების მონაცემებს და ა. შ. ნახ. 7.3 არის საერთო ჰენდლის მონაცემების შენახვის პროცესის სქემატური დიაგრამა. პროცესი ძირითადად მოიცავს ჩაწერას, სინქრონიზაციას და გადამოწმებას. პირველი, ERN აინიცირებს ჰენდლის სერვისის რეგისტრაციის მოთხოვნას რეგისტრაციის კლიენტის მეშვეობით. რეგისტრაციის კლიენტი ახდენს მოთხოვნის კლასიფიკაციას და მას საიდენტიფიკაციო სერვისის კვანძში ან ბლოკჩეინის კვანძში აგზავნის. მეორეც, ISN და ERN მიჰყვებიან ჰენდლის პროტოკოლს, რათა დაასრულონ ავთენტიფიკაცია და UHD რეგისტრაციის პროცესი. კონსორციუმის ბლოკჩეინის ქსელის კვანძები აგროვებენ ტრანზაქციებს,

აწყობენ მათ ბლოკებად და ასრულებენ THD რეგისტრაციას კონსენსუსის აღრიცხვის პროცესის შემდეგ. დაბოლოს, UHD სინქრონიზაცია ხორციელდება ISN-ების DB-ებს შორის. ISN-ებს შეუძლიათ მოითხოვონ სინქრონიზებული UHD-ის მთლიანობის გადამოწმება კონსორციუმის ბლოკჩეინის ქსელის მდგომარეობათა ლეჯერიდან. თუ გადამოწმება ვერ მოხერხდა, იდენტიფიკატორის მონაცემები მოინიშნება, როგორც არანორმალური.

ერთის მხრივ, ეს გადაწყვეტა ახდენს THD-ის და UHD-ის გადამოწმების ინფორმაციის ჩაწერას განაწილებულ ლეჯერში რეგისტრაციის დაწყებიდან, რაც უზრუნველყოფს საერთო ჰენდლის მონაცემთა მთლიანობას შენახვისა და სინქრონიზაციის პროცესში; მეორე მხრივ, საკვანძო მონაცემების განაწილებულ ლეჯერში ჩაწერამ შეიძლება თავიდან აიცილოს მტყუნების ერთი წერტილით გამოწვეული რისკი და გააუმჯობესოს საერთო ჰენდლის მონაცემების ხელმისაწვდომობა.

უფლებამოსილი ჰენდლის შენახვის მექანიზმი: უფლებამოსილი ჰენდლი არის წინაპირობა საწარმოებისთვის, რათა გადაამოწმონ ადმინისტრატორის იდენტურობა და მართონ იდენტიფიკატორი; ასევე არის ნაბიჯი, რომელიც უნდა გადაიდგას საერთო ჰენდლის გარჩევადობისთვის. აქედან გამომდინარე, მეორე დონის კონსორციუმის კვანძი აღრიცხავს უფლებამოსილი ჰენდლის ყველა მონაცემს მდგომარეობათა ლეჯერში.

ნახ. 7.3 წარმოგვიდგენს უფლებამოსილი ჰენდლის მონაცემების შენახვის პროცესის სქემატურ დიაგრამას. მეორე დონის კონსორციუმის კვანძების წევრებს შეუძლიათ წაიკითხონ ლეჯერის მონაცემები და ერთობლივად გააკონტროლონ უფლებამოსილი ჰენდლის მონაცემების ცვლილებები, მაგრამ ჩაწერის ნებართვები თითოეული კვანძისთვის განსხვავებულია.

კერძოდ, საწარმოს კვანძს აქვს უფლება ჩაწეროს საწარმოს პრეფიქსის უფლებამოსილი ჰენდლის მონაცემები და გარკვეული ლოგიკის მიხედვით მართოს მონაცემები ISN-თან ერთად. ISN მართავს ყველა საწარმოს პრეფიქსს და უნდა გასცეს ნებართვა ყველა საწარმოს პრეფიქსის უფლებამოსილი ჰენდლისთვის. NMN პასუხისმგებელია ISN-ების მართვაზე და მას შეუძლია შეცვალოს მათი იდენტიფიკატორის გადამოწმების ინფორმაცია და ჩაწეროს შესაბამისი უფლებამოსილების ჰენდლის მონაცემები. ეს გადაწყვეტა ინახავს უფლებამოსილების ჰენდლის მონაცემებს იდენტიფიკატორის მდგომარეობათა ლეჯერში, რაც ეფექტიანად უშლის ხელს ავთენტიფიკაციის მონაცემებისა და გარჩევადობის მონაცემების გაყალბებას. კორპორაციული იდენტიფიკატორის გადამოწმება ხდება ბლოკჩეინის ქსელის მეშვეობით, რაც თავიდან აგვაცილებს ხელმისაწვდომობის დაზიანებას, რომელიც გამოწვეულია მტყუნების ერთი წერტილით.

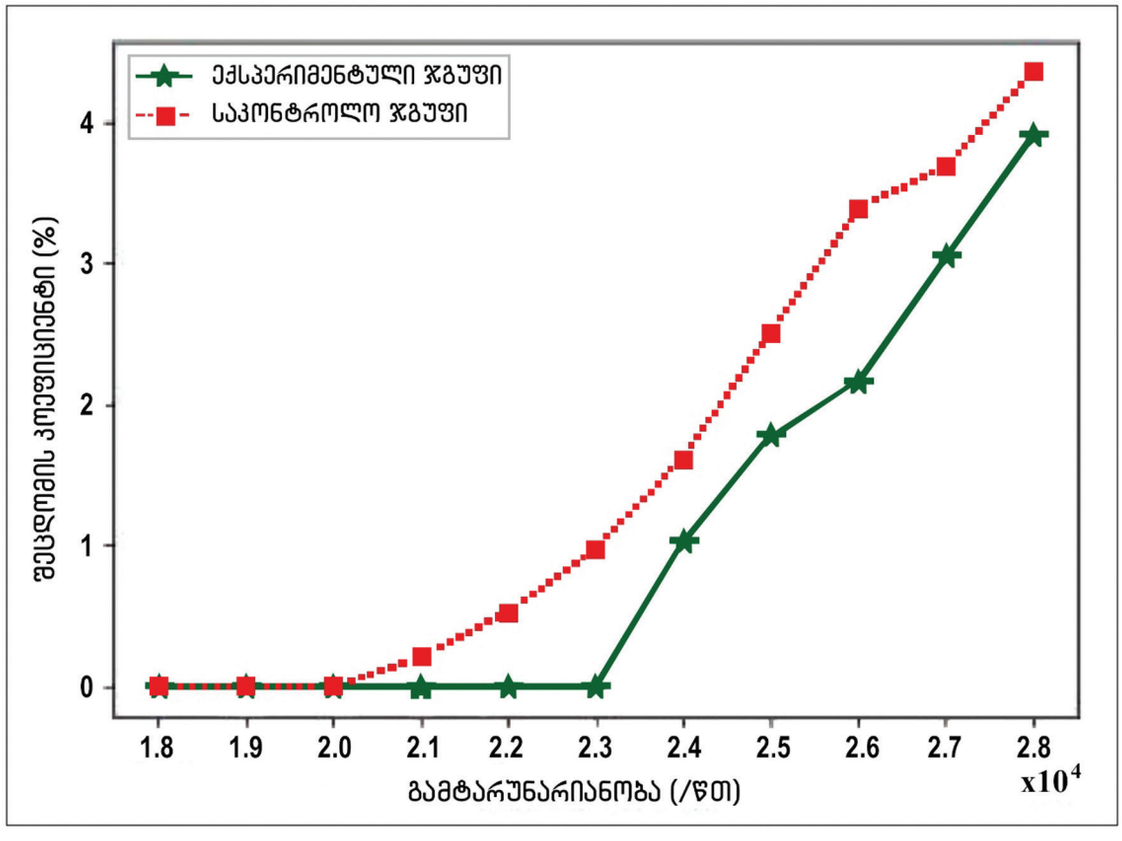
7.5. ექსპერიმენტული შედეგები, დისკუსიები და ღია საკითხები

ამ პარაგრაფში წარმოდგენილია TICA-ის კომპიუტერული სიმულაციით მიღებული მახასიათებლების შეფასება. მოცემული სტრუქტურა დაფუძნებულია ჰიპერლეჯერის სისტემაზე და გამოყენებულია ორი სერვერი მისი ძირითადი კვანძების სიმულაციისთვის. აღებულია TICA-ის ექსპერიმენტული ჯგუფი, რათა შევადაროთ ტრადიციულ ჰენდლზე დაფუძნებულ არქიტექტურას, ანუ საკონტროლო ჯგუფს. ექსპერიმენტული ჯგუფი იყენებს ბლოკჩეინს, მეორე დონის კვანძის გაფართოების მიზნით კონსორციუმის ბლოკჩეინის ქსელში ჰენდლის მემკვიდრეობითი პრობლემების გადასაჭრელად და მახასიათებლების გასაუმჯობესებლად. შედეგები ორი ძირითადი მახასიათებლის კუთხით, ასეთია:

შეცდომის კოეფიციენტი. გარჩევადობის გამტარუნარიანობა განისაზღვრება, როგორც სისტემისთვის მოთხოვნების მაქსიმალური რაოდენობა წამში. პასუხის შეცდომის კოეფიციენტი კონკრეტული გამტა-

რუნარიანობის მიხედვით გამოიყენება არქიტექტურის მუშაობის ეფექტიანობის გასაზომად. გარჩევადობის სერვისის მაღალი ხელმისაწვდომობის უზრუნველსაყოფად, პასუხის შეცდომის კოეფიციენტი თეორიულად 1 პროცენტზე დაბალი უნდა იყოს. ტესტის შედეგები ნაჩვენებია ნახ. 7.5-ზე. ის აჩვენებს, რომ პასუხის შეცდომის კოეფიციენტი იზრდება გამტარუნარიანობის მატებასთან ერთად. როდესაც გამტარუნარიანობა არის წუთში 23000-ჯერ, საკონტროლო ჯგუფის პასუხის შეცდომის კოეფიციენტი დაახლოებით 1 პროცენტია. როდესაც გამტარუნარიანობა არის წუთში 24000-ჯერ, ექსპერიმენტული ჯგუფის პასუხის შეცდომის კოეფიციენტი დაახლოებით 1 პროცენტია. იგივე ერთპროცენტიანი შეცდომის კოეფიციენტით, TICA-ის გამტარუნარიანობა წუთში 1000-ჯერ უფრო მაღალია, ვიდრე ტრადიციული არქიტექტურის.

საშუალო შეყოვნება. საშუალო შეყოვნება განისაზღვრება, როგორც სისტემის მიერ დახარჯული საშუალო დრო სანდო გარჩევადობის დასასრულებლად, რომელიც მოიცავს, როგორც გარჩევადობის, ასევე გადამოწმების დროს. ის ზომავს სისტემის მუშაობის მახასიათებელს, როდესაც უზრუნველყოფს სანდო გარჩევადობის სერვისს. შეცდომის შესამცირებლად, ექსპერიმენტულ ჯგუფსა და საკონტროლო ჯგუფს შორის ჩატარდა 10 ექსპერიმენტის გამეორება. გარჩევადობისთვის ორ ჯგუფს აქვს დაახლოებით ერთნაირი შეყოვნება, რადგან ეს განპირობებულია საერთო ჰენდლის სპეციფიკურობით ამ ორი შემთხვევისთვის. გადამოწმებისთვის, ექსპერიმენტული ჯგუფის შეყოვნება გაცილებით დაბალია, ვიდრე საკონტროლო ჯგუფის, განსხვავებული გადამოწმების მექანიზმების გამოყენების გამო. შედეგი ნაჩვენებია ნახ. 7.6-ზე. შემოთავაზებული არქიტექტურის საიმედო გარჩევადობა გაიზარდა 37 პროცენტით მონაცემთა უსაფრთხოების უზრუნველყოფის წყალობით.

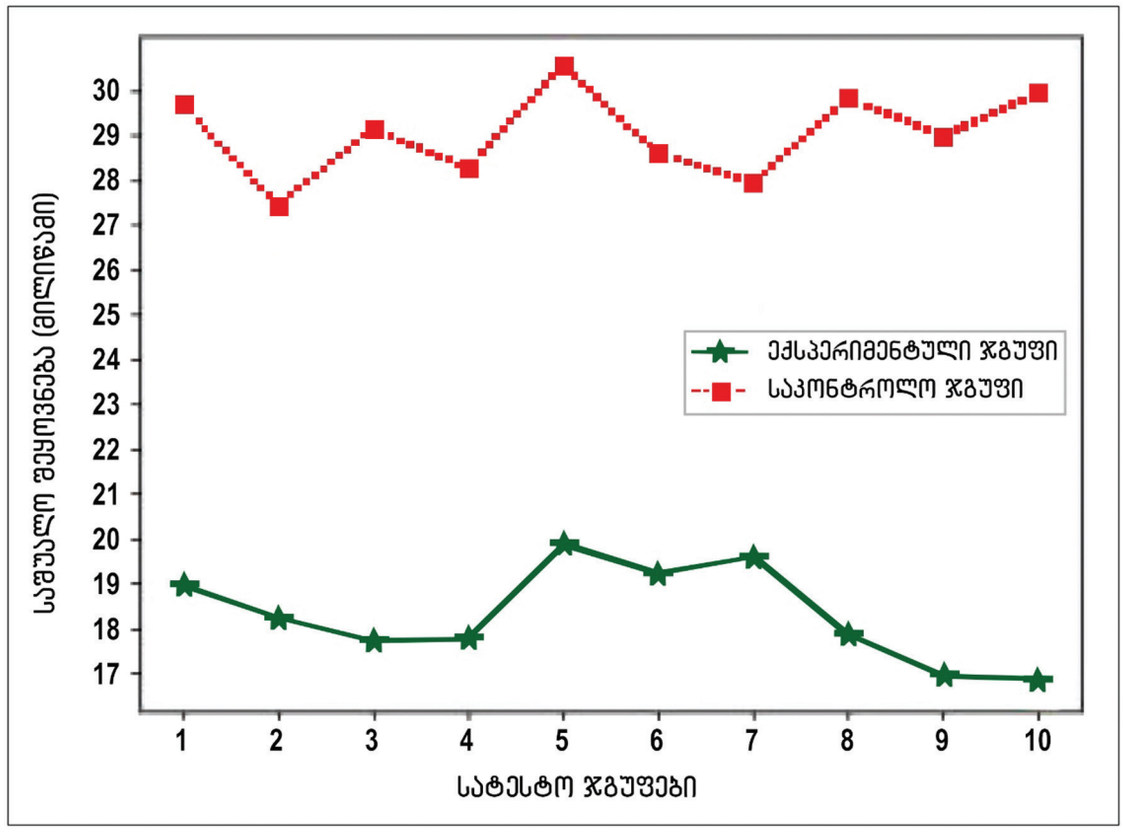


ნახ. 7.5. ტესტირებით მიღებული შეცდომის კოეფიციენტი

პარაგრაფის დასასრულს აღვნიშნავთ, რომ ეს თავი გვთავაზობს სანდო იდენტიფიკატორით ერთობლივი მმართველობის არქიტექტურას ბლოკჩეინის ტექნოლოგიისა და ჰენდლის ტექნოლოგიის გამო-

ყენებით. მიუხედავად იმისა, რომ აქ გადაწყვეტილია ზოგიერთი პრობლემა საიდენტიფიკაციო მონაცემების უსაფრთხოებასთან და მმართველობის სამართლიანობასთან დაკავშირებით, ჯერ კიდევ არსებობს გარკვეული გამოწვევები, რომელთა მოგვარებაც მომავალ კვლევებშია საჭირო:

1. ბლოკჩეინის უსაფრთხოების, მასშტაბურობისა და დეცენტრალიზაციის ერთდროულად მიღწევა შეუძლებელია. ამიტომ, ბლოკჩეინზე დაფუძნებული IIoT-ის იდენტურობის გარჩევადობის სისტემამ ფოკუსირება უნდა მოახდინოს ტრანზაქციის გამტარუნარიანობასა და იდენტიფიკატორის წარმოქმნის სიჩქარეს შორის, და ასევე, შეზღუდული გამტარუნარიანობის მქონე ლეჯერის და იდენტიფიკატორის დიდი რაოდენობით მონაცემებს შორის არსებულ წინააღმდეგობებზე, კონკრეტული სცენარისთვის მკაფიო მოთხოვნების გათვალისწინებით. ასევე, შესაძლებელია განხილულ იქნეს ჯაჭვის სტრუქტურის შეცვლა და კვანტური რეზისტენტული ტექნოლოგიის გამოყენება ბლოკჩეინში ზემოაღნიშნული პრობლემების გადასაჭრელად.
2. იდენტურობის გარჩევადობა არის IIoT-ში მონაცემთა მიმოქცევის წინაპირობა. იდენტიფიკატორებზე დახვეწილი წვდომის კონტროლს შეუძლია სრულად და ეფექტიანად დაიცვას კორპორაციული მონაცემების კონფიდენციალურობა. ამიტომ, ატრიბუტების დაშიფვრის ტექნოლოგიაზე დაფუძნებული იდენტურობის გარჩევადობის კონტროლი შემდგომი კვლევების მიმართულება გახდება.
3. AAS-ის აქვს ორი მნიშვნელოვანი მიზანი, რაც არის ინდუსტრიებს შორის მონაცემთა ურთიერთქმედების რეალიზება და ინფორმაციის ფილტრაციის სირთულის შემცირება. ამიტომ, შემდგომში ასევე, უნდა შევისწავლოთ AAS-ის გამოყენება მონაცემთა მოდელირებისთვის, რათა მიღწეულ იქნეს იდენტურობის გარჩევადობის ინტეგრაცია.



ნახ. 7.6. ტესტირებით მიღებული საშუალო შეყოვნება

7.6. მეშვიდე თავის დასკვნა

ამ თავში ჩვენ შევისწავლეთ სანდო იდენტიფიკატორით ერთობლივი მმართველობის ახალი არქიტექტურა IIoT-სთვის. ასევე წარმოდგენილია ამ სისტემის განხორციელების პროტოტიპი და ნაჩვენებია სისტემის მიზანშეწონილობა და გამოყენებადობა. ექსპერიმენტებმა აჩვენა, რომ შემოთავაზებულმა არქიტექტურამ მიაღწია უკეთეს შედეგებს შეცდომის კოეფიციენტისა და საშუალო შეყოვნების თვალსაზრისით, ტრადიციულ ჰენდლზე დაფუძნებულ არქიტექტურასთან შედარებით. მომავალში, ჩვენ ვიმედოვნებთ, რომ ბლოკჩეინი ასევე გამოყენებული იქნება AAS-ის მეშვეობით IIoT-ის იდენტიფიკატორის გარჩევადობაში. ასევე შესასწავლია იდენტიფიკატორის წვდომის კონტროლი ატრიბუტების დაშიფვრის ტექნოლოგიაზე დაყრდნობით.

თავი 8. უსაფრთხო ვირტუალური მობილური პატარა ფიჭების შემუშავება B5G/6G ქსელებისთვის

8.1. შესავალი

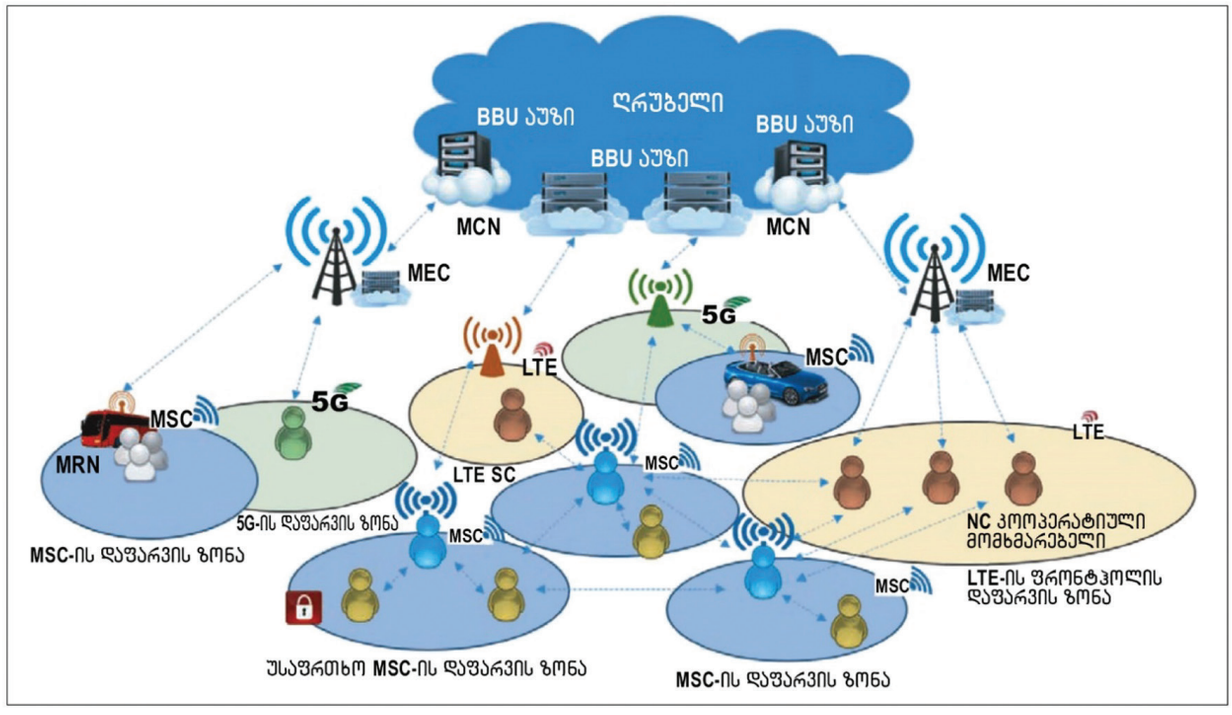
საყოველთაოდ აღიარებულია, რომ 6G-ის ერთ-ერთი ამოცანაა ციფრული ტექნოლოგიებისა და ხელმისაწვდომობის განვითარება, ასევე ეკონომიკური ღირებულებისა და შესაძლებლობების გახსნა სოფლად. 5G ტექნოლოგიით უკვე შემოთავაზებული სერვისების გამოყენებით, 6G მიზნად ისახავს სერვისების კიდევ უფრო მდიდარი ნაკრების ინტეგრირებას, რომელიც მოიცავს, ვირტუალურ და გაფართოებულ რეალობას, ავტონომიურ მანქანებს. ამას დასჭირდება „გამრღვევი“ არქიტექტურები, რომლებსაც შეუძლიათ 5G-ზე დაფუძნებული ბაზრისთვის შესაბამისი გადაწყვეტილებების მიწოდება. ამ კონტექსტში, ძალიან მნიშვნელოვანია SECRET ინიციატივა – ევროპული სასწავლო ქსელი, რომელიც მიზნად ისახავს გადადგას ნაბიჯი 6G ხედვისკენ შემდეგი თაობის საკომუნიკაციო პლატფორმის შეთავაზებით, რომელიც 5G მომხმარებელების დაფარვის არეალს აფართოებს.

SECRET, უფრო კონკრეტულად, SECRET-MSC (იშიფრება, როგორც უსაფრთხო ქსელური კოდირება შემცირებული ენერგიით, შემდეგი თაობის მობილური პატარა ფიჭებისთვის) პლატფორმა, მობილურ ქსელებს საშუალებას აძლევს აღიქვან მობილური მოწყობილობები, როგორც ხელმისაწვდომი ვირტუალური რესურსების აუზი გამოთვლითი, შენახვისა და ქსელური შესაძლებლობებით; ანუ, საბოლოო მომხმარებლები შეიძლება გახდნენ ავტონომიური პატარა ფიჭები, რომლებიც მემკვიდრეობით იღებენ რადიორესურსების მართვის შესაძლებლობებს და მათ მობილური პატარა ფიჭები ეწოდებათ. SECRET კავშირის ლანდშაფტი უზრუნველყოფს MSC-ების უსადენო ქსელს, რომელიც მოიცავს ურბანულ ლანდშაფტს და ის ვირტუალური ხასიათისაა, კონფიგურირებულია მოთხოვნისამებრ, რაც ქმნის საფუძველს ლოკალიზებული პატარა ფიჭების კავშირისთვის. პლატფორმას მართავს განაწილებული SW-ით განსაზღვრული ქსელის არქიტექტურა, რომელიც იყენებს ისეთ ფუნქციებს, როგორიცაა: ქსელის ნაწილებად დაყოფა, ღრუბლოვანი გამოთვლები და საკუთრების მთლიანი ღირებულება (TCO) მობილური ქსელის ოპერატორებისთვის. ყოველივე აღნიშნული 6G ფილოსოფიის განუყოფელი ნაწილია.

ამ კონტექსტში, SECRET იკვლევს დადასტურებულ ტექნოლოგიურ პარადიგმებს, რომლებიც ეფუძნება ქსელის კოდირებულ კოოპერაციას (NCC) და ვირტუალიზაციას. მიუხედავად იმისა, რომ ვირტუალიზაცია ხორციელდება სრულფასოვანი გამოთვლითი ინსტრუმენტების საფუძველზე, როგორიცაა SDN და NFV, დადასტურდა, რომ NCC აუცილებელია დღევანდელი მობილური პარადიგმებისთვის. NCC ორგანიზაციებს ურთიერთქმედებისა და თანამშრომლობის საშუალებას აძლევს გადაცემული სიგნალის ხარისხის გასაუმჯობესებლად, სისტემის მიერ სიხშირის გატარების ზოლის ეფექტიანად გამოყენებისას. ეს ორი პარადიგმა გაერთიანდა 5G-ზე დაფუძნებული ინტეგრირებული არქიტექტურის უზრუნველსაყოფად, 5G-ის, B5G-ის და 6G-ის მოთხოვნილებების შესაბამისი კომუნიკაციის, გამოთვლების, ქეშირების და მენეჯმენტის ოპტიმიზაციის თვალსაზრისით, რომელსაც შეუძლია გააუმჯობესოს TCO ეფექტიანობა, დააკმაყოფილოს შეყოვნებისა და სანდოობის მიზნები. ეს ინტეგრირებული SECRET მიდგომა აჩენს მნიშვნელოვან გამოწვევებს ვირტუალიზაციის, მობილურობის, უსადენო ქსელის უსაფრთხოებისა და ენერგოეფექტიანი RF-ის თვალსაზრისით, რაც 6G ტექნოლოგიის გამოწვევებს შეესაბამება. ეს თავი ყურადღებას ამახვილებს ძირითად ტექნოლოგიებსა და სტანდარტიზაციის ტენდენციებზე, ამ გამოწვევების გადასაჭრელად ვირტუალური MSC-ების დანერგვით, რაც ნაჩვენებია ფიჭის ეფექტიანი და საიმედო გადმოტვირთვის გამოყენებით.

8.2. SECRET-ის ხედვა: მობილური პატარა ფიჭები B5G-სთვის

SECRET-ის ძირითადი სცენარი ითვალისწინებს დინამიკურად შექმნილ MSC-ებს, რომლებიც ვირტუალური ხასიათისაა და მოიცავს შეზღუდულ გეოგრაფიულ არეალს. მათი დაყენება შესაძლებელია ნებისმიერ ადგილას, ნებისმიერ დროს და ნებისმიერ მობილურ (ან ფიქსირებულ) მოწყობილობაზე, რაც დამოკიდებულია ქსელის პირობებზე და მოწყობილობის შესაძლებლობებზე. საბოლოო მომხმარებლის თვალსაზრისით, ეს MSC-ები მხარს უჭერენ ბევრ პოტენციურ 6G სერვისს დაბალ ფასად და ნაკლები ზეგავლენით მობილური ბატარეის მუშაობის ხანგრძლივობაზე. თითოეულ MSC-ს მართავს ფიჭის მობილური თავი (MCH), რომელიც არის მობილური მოწყობილობა კლასტერების იდენტიფიცირებულ კომპლექტში და ნომინირებულია ადგილობრივ რადიო-მენეჯერად. MCH აკონტროლებს და ინახავს აქტიური მომხმარებლების ერთობლიობას ფიჭის დაფარვის ზონაში. როგორც ნაჩვენებია ნახ. 8.1-ზე, MCH-ები თანამშრომლობენ სხვა MSC-ების MCH-ებთან, რათა ჩამოაყალიბონ „პატარა ფიჭების უსადენო ქსელი“, რომელსაც შეიძლება ჰქონდეს რამდენიმე კარიბჭე ან ძირითად მობილურ ქსელთან (MCN) ინფრასტრუქტურაზე დაფუძნებული ქსელის მეშვეობით (4G/5G), ან სხვა მომხმარებლის მოწყობილობებთან, მაგალითად, ფიჭის გადმოტვირთვისთვის.



ნახ. 8.1. SECRET-ის ფუნქციონირების სცენარი (აკრონიმები მოცემულია წიგნის ბოლოს, განყოფილებაში: აბრევიატურები და აკრონიმები)

MSC-ების მთავარი მახასიათებელია ის, რომ ისინი იყენებენ უსადენო ფრონტჰოლისა და ბექჰოლის კავშირებს ღრუბლოვანი RAN-დან (CRAN), MEC კვანძის მეშვეობით MSC-მდე, რითაც თავიდან აიცილებენ მობილურობასთან დაკავშირებულ და ძვირად ღირებული ბოჭკოების განლაგების აუცილებლობას. უსადენო ფრონტჰოლის ლინკს შეუძლია მრავალჯერადი რადიოწვდომის ტექნოლოგიების (MRAT) და ფართო სიხშირული ზოლების მხარდაჭერა, მათ შორის, LTE-სთვის და 5G-სთვის. MSC-ების კიდევ ერთი მახასიათებელია ის, რომ ისინი მობილური მოწყობილობებისთვის გამოიყურებიან,

როგორც სრულფასოვანი BS-ები, როგორიცაა განვითარებული NodeB-ები (eNB), რომლებიც უზრუნველყოფენ ადგილობრივ წვდომას ბექჰოლის კავშირის მეშვეობით საბაზისო სიგნალების ბლოკების (BBU) აუზთან. BBU აუზი არის ვირტუალიზებული კლასტერი. იგი შედგება მრავალი პროცესორისგან და გამოთვლითი კვანძებისგან, რომლებიც ასრულებენ საბაზისო სიგნალების დამუშავების ფუნქციას და ისინი პრაქტიკიდან გამომდინარე, შეიძლება მთელ ქსელში განაწილდეს. შესაბამისად, MCN, MEC სერვერები და MSC შეიძლება ჩაითვალოს გამოთვლით კვანძებად. კომუნიკაცია MCN-დან ქვემოთ, MSC-მდე დაფუძნებულია ფრონტჰოლის, ბექჰოლის და BBU რესურსების ოპტიმალურ ვირტუალიზაციაზე, რომელიც ადაპტირდება UE მოთხოვნებთან, სერვისის დონის შეთანხმებებთან და გამოთვლით დატვირთვასთან.

ამ მიზნით, SECRET სცენარი მიზნად ისახავს RAN-ის ვირტუალიზაციას MSC-ებისთვის, რომლებიც იმართება განაწილებული SDN არქიტექტურით. ასეთი არქიტექტურა იძლევა გამოთვლის, კომუნიკაციის, ქეშირების და კონტროლის (4C – Computation, Communication, Caching, Control) გადაწყვეტილებების ადაპტირებულ განთავსებას მობილურ პატარა ფიჭებში, რაც 4C-ის საშუალებას აძლევს, მიაღწიოს ახალ საზღვრებს დაფარვის, გამტარუნარიანობის, შეყოვნებისა და საიმედოობის თვალსაზრისით. 4C ტექნოლოგიების ჩართვით, SECRET-ს აქვს პოტენციალი განათავსოს „ფართოდ გავრცელებული“ ფუნქციონალური დანაწევრება და ქსელის ნაწილებად დაყოფა 6G-ის გამოყენების შემთხვევების მხარდასაჭერად, როგორიცაა URLLC და კრიტიკული მანქანური ტიპის კომუნიკაციები, ზრდის რა გამოთვლით დაფარვას სერვისის ჩამოტვირთვის ამოცანებისთვის პერიფერიული ღრუბლიდან ახლოს განთავსებულ მოწყობილობებზე, რაც შეესაბამება ტერმინს – ნისლოვანი (mist) გამოთვლები. ეს უზრუნველყოფს ახალ განზომილებას დამატებითი შეყოვნების შემცირების კუთხით, რათა შემცირდეს კომუნიკაციის ხარჯები და დაკმაყოფილდეს თაობებს შორის წარმოქმნილი მოთხოვნები მობილური ოპერატორებისთვის საკუთრების ღირებულების შემცირების თვალსაზრისით. ვირტუალიზაცია მობილურ მოწყობილობას საშუალებას მისცემს, გახდეს ქსელისა და გამოთვლითი რესურსების აუზი, რომელიც შეიძლება გაზიარებულ იქნეს ოპერატორებსა და სერვისებს შორის.

MSC კონცეფციის განხორციელებამ და ქსელების დანერგვამ წარმოშვა მნიშვნელოვანი გამოწვევები მოწყობილობის ვირტუალიზაციის, უსადენო უსაფრთხოებისა და ენერგოეფექტიანი RF-ის თვალსაზრისით, რაც შეიძლება გამოსახული იყოს SECRET საცნობარო სცენარით. მოქნილი ქსელის მისაღწევად, სადაც ენერგეტიკული, სპექტრული და ქსელის გამოყენების ეფექტიანობა აკმაყოფილებს B5G/6G ქსელების მიზნებს, მინიმუმ საჭიროა:

- CRAN, დაფუძნებული SDN-ზე და NFV-ზე ვირტუალიზაციისა და SW-ის მხარდაჭერით;
- HO-ის ენერგოეფექტიანი მართვის მექანიზმები, რომლებიც უმკლავდება დაკავშირებული მოწყობილობების მაღალ მობილურობას, რომლებიც მოქმედებს, როგორც ფიჭის თავები;
- დეცენტრალიზებული უსადენო ქსელის უსაფრთხოების სტრუქტურა, რომელიც აყალიბებს კრიპტოგრაფიულ გასაღებების მასალას მოწყობილობებს შორის თანამშრომლობის კავშირების უზრუნველსაყოფად;
- ენერგოეფექტიანი ან ე. წ. მწვანე სიმძლავრის გამაძლიერებლები (PA), რომლებიც მიზნად ისახავს გააუმჯობესოს ურთიერთკომპრომისი ენერგოეფექტიანობასა და წრფივობას შორის.

ეს ძირითადი ტექნოლოგიური გაუმჯობესებები და MSC-ების ევოლუცია სტანდარტების ფარგლებში აღწერილია შემდგომ პარაგრაფებში.

8.3. მობილური პატარა ფიჭების შემუშავება ქსელის ვირტუალიზაციისა და SW-ის საშუალებით

MSC-ები შემოთავაზებული და შესწავლილი იყო სხვადასხვა კვლევაში, რათა ნაჩვენები ყოფილიყო სარგებლიანობა ქსელში სპექტრის რესურსების განაწილების პრობლემის გადაჭრის კუთხით. მაგალითად, ზედმეტად დატვირთული მაკროფიჭიდან ტრაფიკის გადმოტვირთვით და პროაქტიული ქეშირების გამოყენებით უსადენო ბექჰოლით და სპექტრის გაზიარებით. თუმცა, ვირტუალურ ქსელში 4C ოპტიმიზაციით განსაზღვრულ ჰოლისტიკური გადაწყვეტის ზემოქმედებას ნაკლები ყურადღება მიექცა.

MSC-ების მოთხოვნის შესაბამისად დაყენება სირთულეს მატებს ვირტუალიზებულ ქსელს და საჭირო ხდება რამდენიმე საკითხის მოგვარება. ვინაიდან საბოლოო მომხმარებელი მონაცემებს იღებს არა „ფიქსირებული“ მდებარეობიდან, არამედ „მოძრავი“ გადამცემიდან, სისტემამ უნდა გაითვალისწინოს სიხშირული სპექტრი, მობილურობა და რესურსების მართვა, როგორც მომხმარებლისთვის, ასევე გადამცემისთვის. ქსელის ვირტუალიზაცია საბოლოოდ შეამცირებს შემოთავაზებული სისტემის სირთულეს, რაც საშუალებას მისცემს სხვადასხვა RAT-ს და MNO-ს ერთმანეთს გაუზიარონ რესურსები, გააუმჯობესონ მდგრადობა, გაზარდონ დაფარვა და შეამცირონ შეყოვნება. ის ასევე უზრუნველყოფს ამჟამად არსებული სისტემის მოთხოვნებთან ადაპტირებულ ინფრასტრუქტურას.

ვირტუალიზებულ ქსელში, ფიზიკური ქსელის რესურსები ასახულია SW-ში მდგრადობის გასაუმჯობესებულად და CAPEX/OPEX-ის შესამცირებლად. MSC-ების შემთხვევაში, უნდა მოგვარდეს 4C-სთან დაკავშირებული შემდეგი საკითხები:

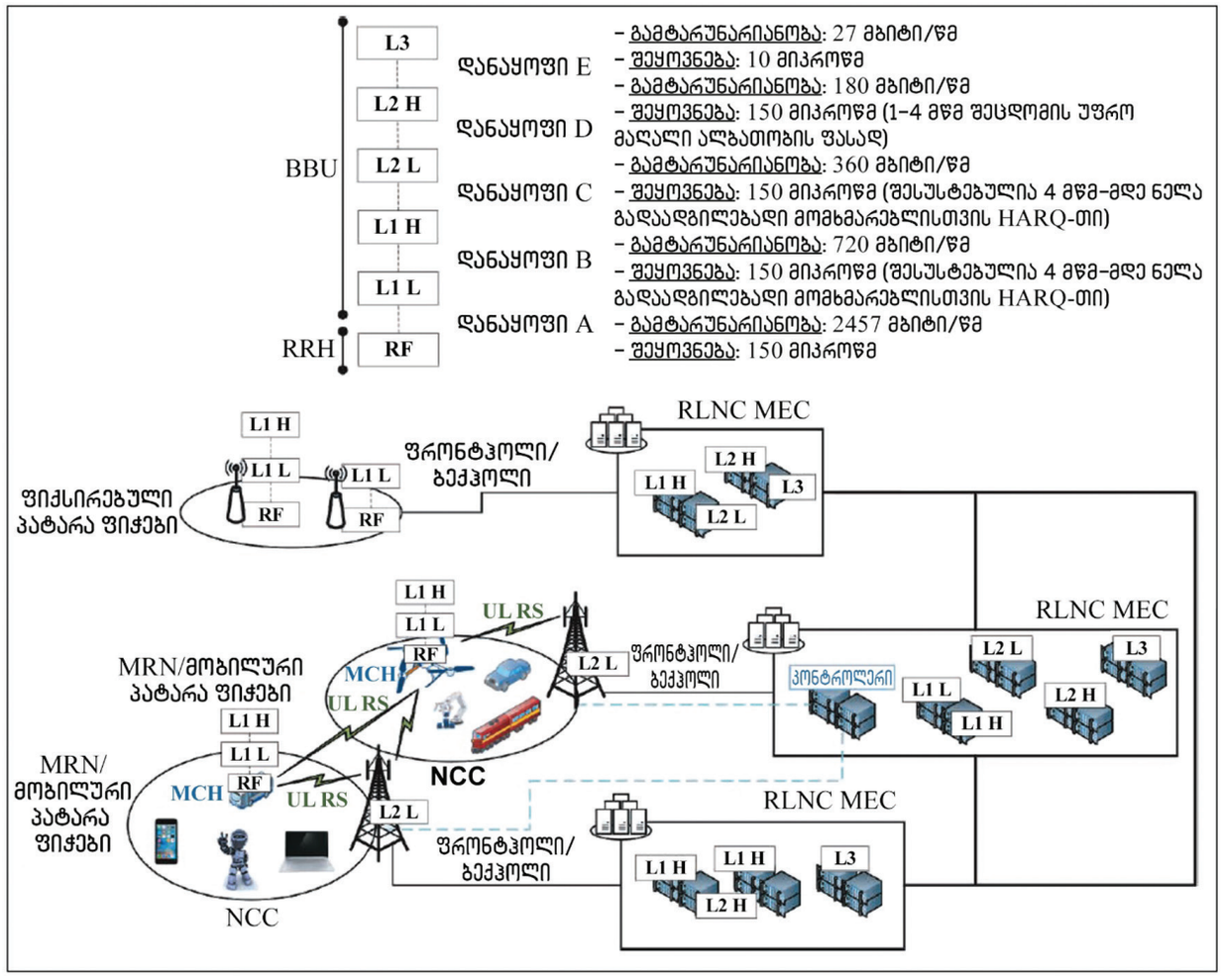
მობილურობის მართვა (MM): MSC-ების განლაგება ზრდის ფიჭის საზღვრებს, რაც პოტენციურად გამოიწვევს HO-ების რაოდენობის გაზრდას მცირე დაფარვის არეალის გამო. უფრო მეტიც, როდესაც MSC-ის სიჩქარე მაღალია, HO-ით განპირობებული სირთულე კიდევ უფრო გაიზრდება, რაც გამოიწვევს ენერგიის მაღალ მოხმარებას გადაჭარბებული HO სიგნალის გამო. აღსანიშნავია, რომ მიმდინარე HO პროცედურები სისტემებში, როგორიცაა 3GPP-ის LTE და 5G, არასაკმარისია მობილურობის ახალი გამოწვევების მოსაგვარებლად, რაც ბიძგს იძლევა სისტემის სრული განახლებისთვის.

რესურსების მართვა (RM): RAN სპექტრი და ინფრასტრუქტურა, პატარა ფიჭების (SC) ჩათვლით, გათვალისწინებულია გაზიარებისთვის რამდენიმე მესამე მხარის სერვისის პროვაიდერებს შორის, რომლებსაც მობილური ვირტუალური ქსელის ოპერატორებს (MVNO) და MRAT RAN-ებს უწოდებენ. ასეთი გაზიარების გააქტიურება მოითხოვს RAN-ების სრულად ვირტუალიზაციას NFV-სა და SDN-ის გამოყენებით RAN ქსელის ფუნქციებში და ქსელურ მოწყობილობებში, შესაბამისად. მიუხედავად იმისა, რომ NFV საშუალებას იძლევა მოხდეს RAN-ის გაზიარება სხვადასხვა მოიჯარის (MVNO) მიერ, ვირტუალური რესურსების მართვის (VRM) ოპერაციები რადიო და გამოთვლითი ფიზიკური კვანძებისთვის საჭიროებს ალგორითმებს, რომლებიც უზრუნველყოფენ გაზიარებული რესურსების დინამიკურ განაწილებას და მოქნილ მართვას SLA-ების და დატვირთვის შესაბამისად, თითოეული MVNO-სთვის. VRM ალგორითმები მოიცავს:

- რადიორესურსების განაწილებას (UE-SC დაწყვილება, სიხშირის გატარების ზოლის განაწილება, UE-SC-ის როლის შერჩევა, ქსელის დახმარებით კონფიგურაცია და ა. შ.);
- საკომუნიკაციო და გამოთვლითი რესურსების საიმედო განაწილებას (მაგალითად, კომუნიკაციები ქსელური კოდირებით (NC), ენერგოეფექტიანი BBU განაწილება).

ფიჭის გადმოტვირთვა (CO): ფიჭის გადმოტვირთვა, რომელიც 4G ან დაბალსიხშირიან 5G ქსელებში ეფუძნება ქსელის ერთი წერტილიდან მეორეში ერთი-ერთზე გადაცემის, ანუ უნიკასტის (unicast) მრავალ სესიას, დადასტურდა, რომ არაეფექტურია, თუ იმავე მდებარეობის მომხმარებლები ითხოვენ ერთსა და იმავე კონტენტს. უფრო ეფექტური მიდგომა იქნება ქვეჯგუფების სისტემა, სადაც UE-ები ორგანიზებულია ჯგუფებად და ინფორმაცია მთელ ჯგუფში, მხოლოდ ერთხელ იგზავნება.

ვირტუალური ქსელი ჩვეულებრივ, ორი ვირტუალური ფენისგან შედგება, რომელსაც ეწოდება საკონტროლო სიბრტყე და მონაცემთა (ან მომხმარებლის) სიბრტყე. საკონტროლო სიბრტყე ძირითადად MM-ს ამუშავებს, ხოლო მონაცემთა სიბრტყე – საკომუნიკაციო რესურსებს. თავის მხრივ, MM მოიცავს ორ მთავარ ქსელურ პროცედურას: HO მართვას (როგორც ჰორიზონტალური, ასევე ვერტიკალური მიმართულებით) და დამუშავების რესურსების მართვას (ანუ გამოთვლითი რესურსების მიგრაციას ხელმისაწვდომ რესურსებს შორის). პირველ შემთხვევაში, HO პროცედურა, რომელიც დაფუძნებულია აპლინკის (UL) საცნობარო სიგნალზე (UL RS) და ნაჩვენებია ნახ. 8.2-ზე, გვთავაზობს მნიშვნელოვან სარგებელს MSC-ებისთვის.



ნახ. 8.2. BBU-ის ლოგიკური დაყოფის წარმოდგენა (ზემოთ) და CRAN-ის ასახვა, რომელიც ეფუძნება ქსელის კოოპერაციულ კოდირებას და მობილურ პერიფერიულ გამოთვლებს. პატარა ფიჭები (ფიქსირებული ან მობილური) კომუნიკაციაში არიან პერიფერიულ მონაცემთა ცენტრებთან (სადაც განთავსებულია ვირტუალური BBU-ების ქვეფენები) ფრონტჰოლის/ბექჰოლის ლინკების მეშვეობით, რომლებიც უნდა აკმაყოფილებდეს დაყოფისთვის ზემოთ მონიშნულ მოთხოვნებს (აკრონიმები მოცემულია წიგნის ბოლოს, განყოფილებაში: აბრევიატურები და აკრონიმები)

MSC გადასცემს UL-ის RS-ს, რომელიც ერთდროულად მიიღება როგორც მომსახურე, ისე მეზობელ მაკრო BS-ებზე. BS-ები ზომავენ UL-ის საცნობარო სიგნალს (RS) და ამ ინფორმაციას უგზავნიან ცენტრალური ქსელის კონტროლერს გაზომვის შემდგომი დამუშავებისთვის, რათა გადაწყვიტოს, რომელი BS მოემსახურება მოცემულ MSC-ს. ამიტომ, გაზომვა და შემდგომი ანგარიშის გადაცემა არ არის საჭირო მობილური მოწყობილობიდან, რაც ამცირებს HO სიგნალს და მასთან დაკავშირებულ ენერგიის მოხმარებას.

მონაცემთა სიბრტყე ძირითადად, დაკავშირებულია RM-თან, რომელიც მომავალი CRAN-ების კიდევ ერთი ძირითადი ფუნქციაა. მემკვიდრეობითი CRAN გადაწყვეტილებები, ვირტუალური BBU დაყოფის გათვალისწინებით, უზრუნველყოფს ლოგიკური დაყოფის ხუთ ძირითად შესაძლებლობას მათი სპეციფიკური მოთხოვნებით (ნახ. 8.2). ვირტუალური BBU-ების ლოგიკური ქვეფუნქციები დაფუძნებულია SW-ზე (ანუ მუშაობს ვირტუალურ მანქანებში, კონტეინერებში და ა. შ.). ისინი დინამიკურადაა მოთავსებული სხვადასხვა სერვერში ან პერიფერიულ მონაცემთა ცენტრებში, ან ჩაშენებულია მობილური მომხმარებლების შიგნით (როდესაც გამოთვლითი დატვირთვა ხელმისაწვდომია). ასეთი რესურსები კონკრეტულ მონაცემთა ცენტრებში დაცულია მომხმარებელთა მობილურობის მახასიათებლების, წარმატებული და საიმედო კომუნიკაციის მოთხოვნების შესაბამისად. კომუნიკაცია სერვერებს შორის, რომლებიც მიეკუთვნებიან იმავე ან სხვადასხვა მონაცემთა ცენტრს, უზრუნველყოფილია ქსელური კოდირებით. კერძოდ, NC შეიძლება ეფექტიანად იქნეს გამოყენებული, როგორც ქსელური პროტოკოლი ვირტუალური BBU-ების ქვეფუნქციების დასაკავშირებლად და განაწილებული გამოთვლებისა და შენახვის საიმედოობის გასაუმჯობესებლად.

NC-ზე დაფუძნებული ქვეჯგუფების სქემებისთვის შესაძლებელი განლაგების უზრუნველყოფა მოითხოვს მოქნილ არქიტექტურას, რომელსაც შეუძლია მყისიერად განათავსოს MSC-ები, სადაც საერთო ვიდეომოთხოვნის მქონე UE-ებს ადგილობრივად თანამშრომლობა შეუძლიათ. ამ კონტექსტში, SECRET საკომუნიკაციო ინფრასტრუქტურა გვთავაზობს ფიჩის გადმოტვირთვის პრაქტიკულ გადაწყვეტას, რომელიც ამცირებს ენერგიის მთლიან მოხმარებას და სადაც NCC ეფექტიანად ინახავს და ავრცელებს მონაცემებს MSC-ებში ფიჩური ტრაფიკის გადმოტვირთვით. კერძოდ, MCH აწარმოებს ქვედა ფენის ვირტუალურ BBU ქვეფუნქციებს, ხოლო ზედა ფენები გადმოიტვირთება NCC-ის გამოყენებით. ასეთ გადმოტვირთვას ასევე შეუძლია გამოიყენოს ფიჩათაშორისი თანამშრომლობა სხვადასხვა MCH-ს შორის. უფრო მეტიც, იმის გათვალისწინებით, რომ მოკლე დიაპაზონის ანტენები მოიხმარენ ნაკლებ ენერგიას, ვიდრე მაკროანტენები, ასევე მცირდება ფაილის გადაცემისა და მიღებისთვის მოხმარებული სიმძლავრე. მოკლე მანძილზე მოქმედ ტექნოლოგიებს (მაგალითად, WiFi-ის) შეუძლია უფრო სწრაფი საკომუნიკაციო ლინკები უზრუნველყოს, რაც სისტემის საერთო გამტარუნარიანობას გაზრდის. როგორც ნაკლი, NCC ასევე ამატებს სირთულეს და შეყოვნების ოვერჰედს ქსელში კოდირებისა და სარელეო გადაცემის ოპერაციების გამო. NCC პროტოკოლი მოიცავს ორ განსხვავებულ ფაზას: ფიჩურ და კოოპერაციულს, რომელიც შეიძლება განხორციელდეს მიმდევრობით ან პარალელურად. პირველი არის ფიჩური ფაზა, რომელშიც BS ანიჭებს ინდექსს ყველა UE-ს, რითაც ქმნის კოოპერაციულ ღრუბელს. ის ავრცელებს პაკეტებს (წინასწარ კოდირებულს, გამგზავნთან) მობილურ მომხმარებლებზე უნიკასტის რეჟიმში და იყენებს მულტიპლექსირებას დროითი დაყოფით (TDM) მრგვალი რობინის (ანუ ციკლური გადარჩევის) პროცედურაში. შემდეგი არის კოოპერაციული ფაზა, რომელშიც გამოიყენება ალგორითმი – მრავალჯერადი წვდომა დროითი დაყოფით (TDMA) და რომლის დროსაც თითოეული მობილური მომხმარებელი პასუხისმგებელია მიღებული პაკეტების გადანაწილებაზე კოოპერაციულ ღრუბელში დარჩენილ კვანძებზე. თითოეული UE ხელახლა დააკოდირებს მიღებულ პაკეტებს ამ თაობის კუთვნილი ყველა პაკეტის ინფორმაციის გამოყენებით და გადასცემს ახალ გადაკოდირებულ პაკეტებს დანარჩენ კოოპერაციულ კვანძებში, მოკლე მანძილზე მოქმედი კომუნიკაციის გამოყენებით.

8.4. უსაფრთხოების უზრუნველყოფა მობილური პატარა ფიჭებისთვის

გათვალისწინებულ SECRET სცენარებში კონფიდენციალური ინფორმაცია ჩამოიტვირთება, აიტვირთება და დამუშავდება MSC-ების ქსელის მეშვეობით და გადაიცემა გარე კვანძების გამოყენებით; აქედან გამომდინარე, ძალიან მნიშვნელოვანია ქსელის არქიტექტურის შემუშავება უსაფრთხოების საკითხების ჩართვით.

MSC-ები უსაფრთხოების სერიოზულ პრობლემებს ქმნიან. კრიპტოგრაფიული უსაფრთხოების გადაწყვეტილებებს ამ პრობლემების გადაჭრა შეუძლია, ვინაიდან ისინი მხარდაჭერილი არიან გასაღების მართვის (KM) ეფექტიანი და საიმედო სქემით. KM სქემა კარნახობს კრიპტოგრაფიული გასაღებების ორგანიზებას ქსელის მომხმარებლებს შორის კომუნიკაციის ეფექტიანად უზრუნველსაყოფად. MSC-ის უსაფრთხოების უზრუნველყოფა გულისხმობს შემდეგი მოთხოვნების შესრულებას:

1. **უსაფრთხოება,** რომ მავნე მომხმარებლებმა ვერ გააკონტროლონ ქსელის ნაწილი;
2. **დაკავშირება,** უსაფრთხო არხების დასამყარებლად ნებისმიერ დაკავშირებულ მომხმარებლებს შორის;
3. **მდგრადობა,** მაღალი დონის უსაფრთხოების უზრუნველსაყოფად და KM-ის საშუალებით კომუნიკაციისათვის;
4. **სამართლიანობა,** რომ თანაბრად გადანაწილდეს დატვირთვა ქსელის მომხმარებლებს შორის და თავიდან იქნეს აცილებული ეგოისტური ქცევა.

ზოგადად, KM სქემები ეყრდნობა საიმედო და უსაფრთხო ცენტრალიზებულ სანდო მესამე მხარეს (TTP), მაგრამ ექვემდებარება DoS თავდასხმებს და ფიზიკურ კომპრომისს. ამიტომ, უსაფრთხოება გარანტირებული უნდა იყოს სანდოობის დეცენტრალიზებული KM სქემის გამოყენებით.

პოპულარული გადაწყვეტა მოიცავს სერტიფიკატების ჯაჭვებს და საშუალებას აძლევს ნებისმიერ ორ მომხმარებელს, ვისაც სურს უსაფრთხოდ კომუნიკაცია, მაგრამ არ გააჩნია წინასწარ არსებული ნდობის ურთიერთობა, იპოვონ არსებული სანდო ურთიერთობების ჯაჭვი, რომელიც მათ ერთმანეთთან დააკავშირებს. ამ გადაწყვეტას აქვს უსაფრთხოების სერიოზული ნაკლოვანებები იმის გამო, რომ სანდოობა გარდამავალია და ძირითადად, კონტექსტისგან დამოუკიდებელი. ასევე, მომხმარებლებს სანდოობის ჯაჭვის გარეშე არ შეუძლიათ უსაფრთხო კავშირის დამყარება.

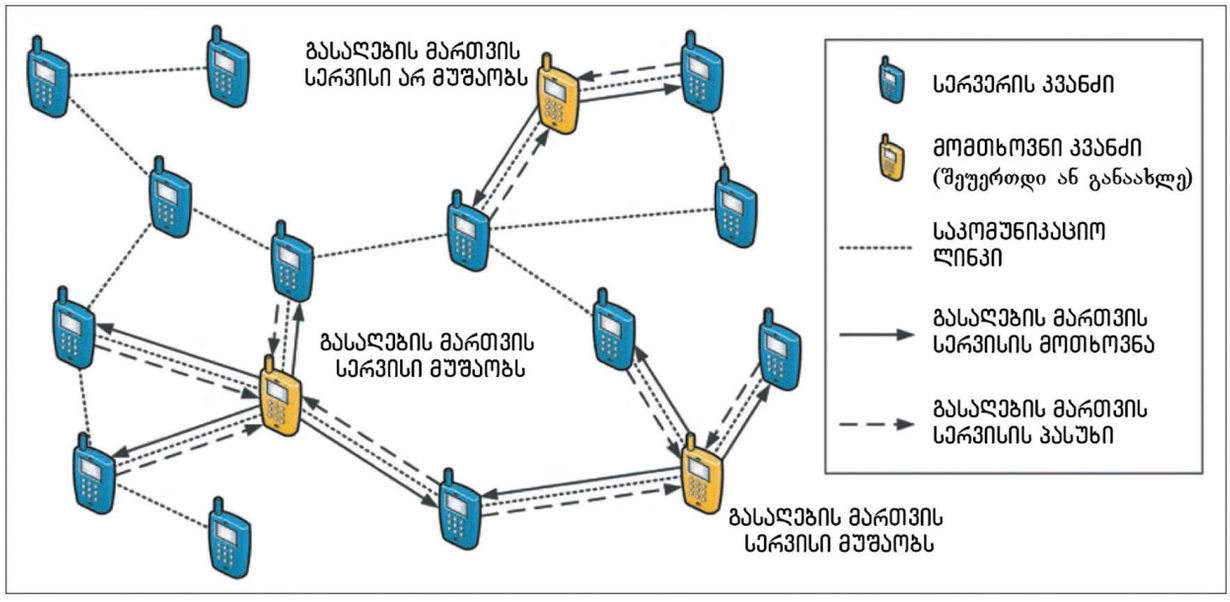
ალტერნატიული გადაწყვეტილებები მოიცავს TTP-ის განაწილებას. ჩვეულებრივ, ცენტრალიზებული TTP უზრუნველყოფს KM სერვისებს ძირითადი გასაღების წყვილის გამოყენებით. თუმცა, ნაწილობრივ განაწილებული TTP (PD-TTP) მიდგომით, გამოსავალი ეყრდნობა ზღურბლის საიდუმლო გაზიარებას, რათა გაიყოს ძირითადი გასაღები გაზიარებულ რესურსებად, რომლებიც ნაწილდება მომხმარებელთა შერჩეულ ჯგუფზე, რომელსაც ეწოდება სერვერები. შესაბამისად, თანამშრომლობით, მათ შეუძლიათ უზრუნველყონ KM სერვისი. ამრიგად, ძირითადი დატვირთვა ამ სერვერებზე მოდის. გარდა ამისა, ისინი შეიძლება არ იყვნენ შეერთების კვანძების გადაცემის დიაპაზონში და დროთა განმავლობაში შესაძლოა მთლიანად დატოვონ ქსელი. ეს საკითხები იწვევს KM სერვისების დროებით ან თუნდაც, მუდმივ მიუწვდომლობას. დაბოლოს, არსებობს სრულად განაწილებული, TTP-ზე დაფუძნებული გადაწყვეტა (FD-TTP), რომელიც PD-TTP-ის მსგავსია, გარდა იმისა, რომ თითოეული კვანძი იღებს ძირითადი პირადი გასაღების წილს (კვანძების შეერთების ჩათვლით). ამრიგად, ამ გადაწყვეტას შეუძლია გადაჭრას PD-TTP-ზე დაფუძნებულ გადაწყვეტაში არსებული პრობლემები. სამწუხაროდ,

თავდაპირველად შემოთავაზებულ გადაწყვეტაში, შეერთებულ კვანძებს არ შეუძლიათ გადაამოწმონ, არის თუ არა განაწილებული KM სერვისი სანდო.

აქედან გამომდინარე, KM სქემის დიზაინი უნდა აკმაყოფილებდეს ყველა შემოთავაზებულ მოთხოვნას და შეფასდეს უსაფრთხოების დონისა და ოვერჰედების (ანუ კომუნიკაციის, გამოთვლითი და მეხსიერების ოვერჰედების) საფუძველზე.

დადგინდა, რომ სერტიფიკატების ჯაჭვსა და PD-TTP-ზე დაფუძნებულ გადაწყვეტილებებს აქვთ თანდაყოლილი დიზაინის ხარვეზები, ხოლო FD-TTP დაფუძნებული გადაწყვეტილებები გადაჭრადია. ამრიგად, ამ თავში შემოთავაზებული, სანდო ცენტრზე დაფუძნებული გასაღების მართვის სქემა შეესაბამება FD-TTP მიდგომას. ეს სქემა იყენებს თვითგენერირებული სერტიფიკატის საჯარო გასაღების კრიპტოსისტემას, მისი უნარის გამო უზრუნველყოს უმაღლესი დონის სანდოობა FD-TTP-ის მიმართ და დაბალი საკომუნიკაციო ოვერჰედის მოთხოვნები სერტიფიკატის არაინტერაქტიული განახლების გამო. იგი შედგება ორი ფაზისაგან, რომლებიცაა: ქსელის ინიციალიზაციის და ოპერატიული ფაზა.

ქსელის ინიციალიზაციის ფაზაში, TTP ინიცირებას უკეთებს ქსელის მომხმარებელთა საწყის კომპლექტს, რაც მათ ძირითადი პირადი გასაღების წილით უზრუნველყოფს. ასევე, მათ ზღურბლურ რაოდენობას საშუალებას აძლევს, ქსელის მუშაობის დროს უზრუნველყონ KM სერვისები (ნახ. 8.3):



ნახ. 8.3. *ქსელის ილუსტრაცია, რომელიც შეიცავს 13 ქსელის კვანძს და 3 გასაღების მართვის სერვისის მოთხოვნის კვანძს. მომთხოვნი კვანძები საჭიროებენ მინიმუმ (ზღურბლური რაოდენობა) 3 ქსელური კვანძის დახმარებას გასაღების მართვის სერვისის წარმატებისთვის*

1. მომთხოვნი კვანძისთვის მისი უფლებამოსილების გასაღების წყვილის მიწოდება, რაც საშუალებას აძლევს, ხელი მოაწეროს თვითგენერირებულ სერტიფიკატებს, თითქოს ისინი ხელმოწერილი იყოს TTP-ის მიერ;
2. მომთხოვნი კვანძისთვის მთავარი პირადი გასაღების უნიკალური წილის მიწოდება და მისი FD-TTP ჯგუფთან მიერთება.

ქსელის მუშაობის დროს, მობილურ კვანძებს შეუძლიათ შეუერთდნენ ქსელს, დამოუკიდებლად გამოიმუშაონ სერტიფიკატები (მოთხოვნისამებრ) და გაცვალონ ეს თვითგენერირებული სერტიფიკატები უსაფრთხო საკომუნიკაციო არხების დასამყარებლად.

8.5. მწვანე RF SECRET-ით მხარდაჭერილი ტელეფონებისთვის

5G რადიოტრანსივერის მუშაობის პრინციპი ფოკუსირებულია ინტეგრაციის მაღალ დონეზე და ენერგოეფექტიანობაზე ბატარეით მომუშავე მოწყობილობებში. კერძოდ, დაბალი ძაბვის ოპერაციებში, ბატარეის ერთ დატენვაზე საუბრის დროის ოპტიმიზაციისთვის, კვლევა ფოკუსირებულია სიმძლავრის გამაძლიერებლების საშუალო ეფექტიანობის შემდგომ გაზრდაზე, რომლებიც იდენტიფიცირებულია, როგორც სიმძლავრის ყველაზე მეტად შთანმთქმელი RF მოდულები. წრფივი გამაძლიერებლების კლასებისთვის მიწოდების ფიქსირებული ძაბვა ამცირებს საშუალო ეფექტიანობას 30 პროცენტს ქვემოთ სუბ-6 გჰც-ის და 20 პროცენტს ქვემოთ მილიმეტრული ტალღების სიხშირეებზე, ხოლო მწვანე PA-ების საშუალო ეფექტიანობა მოსალოდნელია გაუმჯობესდეს 40 პროცენტით, მისაღები 5G სისტემებისთვის. ამიტომ, მონაცემთა უფრო მაღალი სიჩქარისა და უფრო ფართო სიხშირული დიაპაზონის მზარდი მოთხოვნების დასაკმაყოფილებლად, საჭიროა ახალი დაბალფასიანი, ენერგოეფექტიანი და ფართოზოლოვანი ტელეფონების PA-ები, რომლებიც შეამსუბუქებს თერმული გაგრილების პრობლემებს და გააუმჯობესებს MSC-ების მონაცემთა გამტარუნარიანობას.

დინამიკური დატვირთვის მოდულაცია, რომელიც იყენებს უ. დოჰერტის მიერ შემუშავებულ სიმძლავრის გამაძლიერებელს (DPA), არის ერთ-ერთი დომინანტური არქიტექტურა ეფექტიანობის გაუმჯობესების მეთოდებს შორის. სიმძლავრის მაღალი დანაკარგების დროს, მისი გაუმჯობესებული ეფექტიანობის გამო, DPA ფართოდ გამოიყენება, როგორც ფიჭურ საბაზო სადგურებში, ასევე მობილურ მოწყობილობებში მაღალი კრესტ-ფაქტორით მოდულირებული სიგნალების გასაძლიერებლად (კრესტ-ფაქტორი არის არის განსხვავება დეციბელებში სიგნალის პიკურ და საშუალო დონეებს შორის). თუმცა, DPA-ის გამოყენების მთავარი ნაკლი მდგომარეობს მის არაწრფივ დამახინჯებაში და სიხშირის გატარების ზოლის შიდა შეზღუდვაში. ვრცელი კვლევა ჩატარდა DPA-ების ამ მახასიათებლების გასაუმჯობესებლად, რომელიც ფარავს მრავალზოლიან სიხშირეებს მილიმეტრულ ტალღებამდე. ვიწროზოლიან გადაწყვეტილებებზე დაყრდნობით იყო მცდელობები, რათა გაეუმჯობესებინათ საშუალო ეფექტიანობა მისი წრფივობის დარღვევის გარეშე; მათ შორის იყო კარიბჭის წანაცვლების ადაპტაცია, სიგნალის მომვლების თვალყურის დევნება, მრავალარხიანი/მრავალსაფეხურიანი და გაფართოებული რეზონანსული DPA-ების გამოყენება. მიუხედავად იმისა, რომ ამ მიდგომების უმეტესობა უზრუნველყოფს შესანიშნავ მახასიათებლებს, ჰარმონიული დარეგულირების სტრატეგიები E, F და J კლასების გამოყენებით და გაჯერებული DPA-ები ოპტიმალურ გადაწყვეტილებებად იქნა განსაზღვრული. გარდა ამისა, რამდენიმე ძალისხმევა განხორციელდა DPA-ების სიხშირის გატარების ზოლის გაფართოებაზე, ძირითადად, ანალოგური დიზაინის მეთოდოლოგიებში; მათ შორის, სიხშირული მახასიათებლის ოპტიმიზაცია; ასევე, განაწილებული, ტრანსფორმატორის გარეშე, დუალური შესასვლელით და შემდგომ შეთანხმებული DPA-ების გამოყენება. თუმცა, ფართოზოლოვანი DPA-ების უმეტესობა შემუშავებულია 6 გჰც-მდე სიხშირის და დისკრეტული სქემებისთვის და არ შეიძლება გამოყენებულ იქნეს ინტეგრალური სქემების (IC) დანერგვის პროცესში.

5G UE-ის გათვალისწინებით, საჭიროა მაღალი გაძლიერების კოეფიციენტის უზრუნველყოფა, კომპაქტური ზომა, მაღალი სამუშაო სიხშირე და საიმედოობა. ამ კონტექსტში, მონოლითურ მიკროტალღურ IC (MMIC) ტექნოლოგიას შეუძლია გადალახოს ზომის შეზღუდვა და ამავე დროს, გააუმჯობესოს წრფივობა, ეფექტიანობა და გარდამქმნელის გაძლიერების კოეფიციენტი. სრულად ინტეგრირებულ MMIC PA-ში, ყველა პასიური თუ აქტიური კომპონენტი გაერთიანებულია და დანერგილია, როგორც მთლიანი სუბსტრატის მცირე ნაწილები, რათა უზრუნველყოს მოწყობილობის მაღალი იზო-

ლაცია და დაბალი დიელექტრიკული დანაკარგი. უფრო მეტიც, გალიუმის არსენიდი (GaAs) არის სასურველი მასალა მილიმეტრული ტალღების სიხშირეებზე, ძირითადად მისი ელექტრონების მაღალი მობილურობის გამო, რაც გულისხმობს ელექტრონის უფრო მაღალ მიმართულებით სიჩქარეს მოცემული ელექტრული ველისთვის. GaAs-ზე დაფუძნებული საველე ეფექტის ტრანზისტორი არის მომწიფებული, ფასის მიხედვით მისაღები ტექნოლოგია, რამაც გამოიწვია მისი ფართო გამოყენება ფიჭური კომუნიკაციის ბაზარზე.

ბოლო პერიოდში მიღებული და გამოქვეყნებული ექსპერიმენტული შედეგების შედარებით, GaAs ელექტრონების მაღალი მობილურობის ფსევდომორფული ტრანზისტორის (pHEMT) PA-ები უზრუნველყოფს შესანიშნავ მახასიათებლებს გამომავალი სიმძლავრისა და ბექოფის (backoff) ეფექტიანობის თვალსაზრისით. SECRET-ში გამოყენებული იქნა 0.25 მიკრომეტრიანი InGaAs/GaAs (E-რეჟიმის) pHEMT ტექნოლოგია, რომელიც იდეალურად შეეფერება 5G მობილური ტელეფონის PA-ებს კვების დადებითი ძაბვით, რათა უზრუნველყოს ულტრა კომპაქტური MMIC DPA-ის შემუშავება. შემოთავაზებული სიმეტრიული დიზაინის ტექნიკა ეფუძნება ფართოზოლოვანი J კლასის გაძლიერების რეჟიმს. J კლასის PA, რომელიც ახდენს ჰარმონიკების გენერირებას, იყენებს დატვირთვის მეორე ჰარმონიკის ტევადურ კომპონენტებს პარაზიტული ხელშეშლების შთანთქმისთვის, რომლებსაც შეუძლიათ გაზარდონ ძირითადი ძაბვა და ასევე, გაზარდონ ეფექტიანობა. გარდა ამისა, გამოყენებული ფართოზოლოვანი ქსელი შემდგომი შეთანხმებით ამცირებს ჩვეულებრივი DPA-ის იმპედანსის (სრული წინაღობის) ტრანსფორმაციის კოეფიციენტს და აღადგენს სათანადო დატვირთვის მოდულაციას.

8.6. მობილური პატარა ფიჭების დემონსტრირება: SECRET-ის საცდელი სტენდი

SECRET მიდგომა შემოწმდა საცდელი სტენდის საშუალებით, რომელიც ილუსტრირებულია ნახ. 8.4-ზე. საცდელ სტენდს აქვს ორი კარგად დიფერენცირებული ფენა, კერძოდ: HW-ის და ვირტუალიზებული ფენა. საცდელი სტენდი იყენებს SDN-ს ვირტუალიზებულ ფენაში ორი განსხვავებული დაკვირვებადი სიბრტყით, კერძოდ: მონაცემთა და საკონტროლო სიბრტყით.

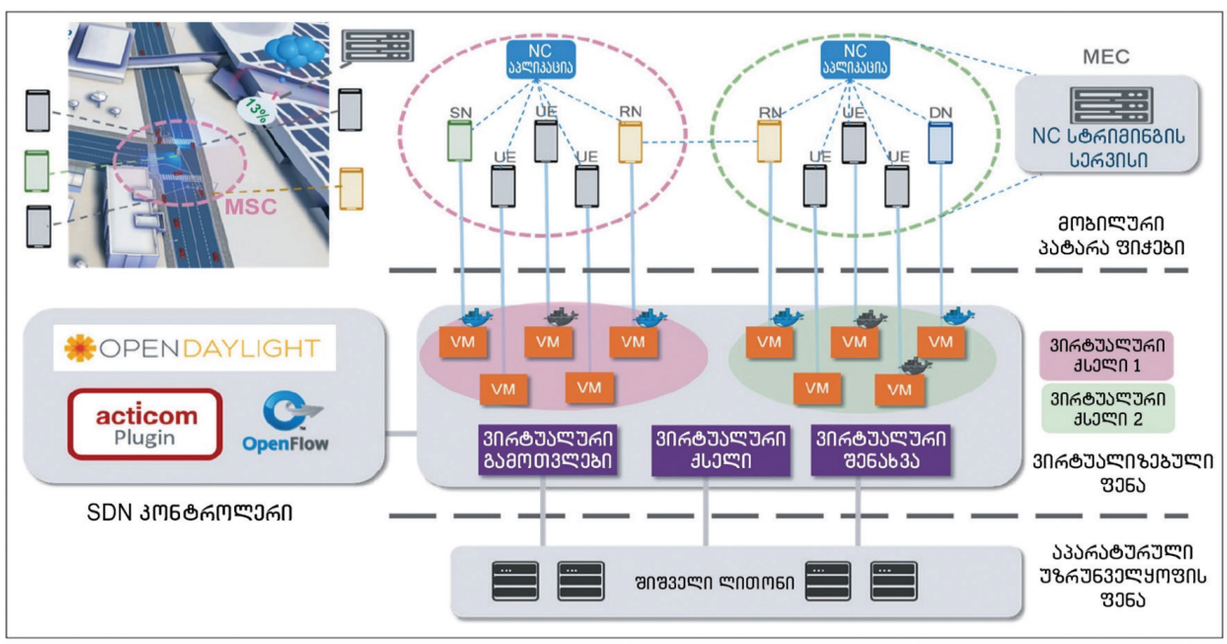
HW-ის ფენა შედგება HP Prodesk 600 G1-ისგან, რომელიც ახდენს სხვადასხვა ფიჭური eNB-ის და სამი Fujistu MPC3-ის ემულაციას (მიბაძვას), რომლებიც ქმნიან ვირტუალიზებულ MSC-ებს (vMSC) და მათში არსებულ UE-ებს. ყველა მათგანი დაკავშირებულია ინტერნეტთან TP-Link C9 როუტერის საშუალებით.

ვირტუალური ფენის საკონტროლო სიბრტყე პროგრამირებადია და იმართება SDN კონტროლერის მიერ. საცდელი სტენდის ძირითადი კომპონენტებია ღია სტეკის (Openstack) ღრუბლოვანი პლატფორმა ქსელის ფუნქციების მართვისთვის და OpenDayLight პროექტით შემუშავებული SDN კონტროლერი ქსელის ნაკადების მართვისთვის. დაყენებისას, ორკესტრატორი იყენებს ღია სტეკის აპლიკაციის პროგრამირების ინტერფეისებს (API) ვირტუალური MSC ფუნქციების გასაშვებად და ავალებს SDN კონტროლერს, მართოს ნაკადები. VM-ები იქმნება გამოთვლით კვანძზე, რომელიც მოქმედებს როგორც UE-ები (ვირტუალური ობიექტები). ბირთვზე (kernel) დაფუძნებული VM, რომელიც არის სრული ვირტუალიზაციის გადაწყვეტა Linux-სთვის x86 აპარატურაზე, გამოიყენება, როგორც ჰიპერვიზორი გამოთვლით კვანძზე VM-ების მასპინძლობისთვის. საცდელ სტენდზე განვიხილავთ MSC-ს, რომელიც განთავსებულია, როგორც გადაფარვის (overlay) ქსელი (გადაფარვის ქსელი არის ვირტუალური ან ლოგიკური ქსელი, რომელიც იქმნება არსებული ფიზიკური ქსელის თავზე). ივარაუდება, რომ MEC სერვერი განლაგებულია eNB-ზე და NC სტრიმინგის სერვისი მუშაობს MEC-ში. შემოთავაზებული მიდგომა ეფუძნება გადაფარვის ქსელს, რომელიც ლოგიკურად აკავშირებს MSC-ში მონაწილე ყველა UE-ის ფიზიკურ

ქსელთან. თითოეული ვირტუალური UE იდენტიფიცირებულია MAC მისამართით, რათა უზრუნველყოს კომუნიკაცია ვირტუალურ UE-ებს შორის გადაფარვის ქსელში. SDN-ზე დაფუძნებული ქსელი უზრუნველყოფს გადაფარვის ქსელის იზოლირებას ღია ნაკადის (OpenFlow) წესების მეშვეობით.

ვირტუალიზებული ქსელის მონაცემთა სიბრტყე შედგება NCC სტრიმინგის სერვისისგან, რომელიც მოთავსებულია MEC-ში, მრავალი MSC-სგან, რომლის კონტროლერი მოთავსებულია MCH-ში და NCC აპლიკაციებისაგან, რომლებიც მოთავსებულია UE-ებში. ვიდეონაკადი გადაიცემა სერვერიდან UE-ებში, რათა აჩვენოს ტრაფიკის გადატვირთვა და გაზრდილი გამტარუნარიანობა.

დემონსტრატორში MSC მოთავსებულია სასწრაფო დახმარების მანქანაში, რომელიც მუშაობს, როგორც MCH. დოკერის კონტეინერი მუშაობს კვანძებში, რათა აჩვენოს, არის თუ არა კვანძი აქტიური, არააქტიური ან ლოდინის რეჟიმში. სასწრაფო დახმარების მანქანაში MSC განტვირთავს ფიჭურ ტრაფიკს და აღწევს 13 პროცენტ ფიჭურ მოხმარებას (ნახ. 8.4). ის მოქმედებს, როგორც შუალედური კვანძი მიმდებარე მანქანებსა და eNB-ს შორის. ვიდეოსტრიმინგის გაშვებამ შეიძლება უზრუნველყოს სანდო კომუნიკაციის საათები დეკოდირების 99.5 პროცენტზე მეტი კოეფიციენტით, რაც შეიძლება კიდევ უფრო გაიზარდოს MSC-ში კოდირებული გადაცემის რაოდენობის გაზრდით. NCC-ის დახმარებით შექმნილი ვიდეონაკადი შესაძლოა, მომგებიანი იყოს სერვისების უზრუნველსაყოფად გამტარუნარიანობის, შეყოვნებისა და საიმედოობის მოთხოვნებით (მაგალითად, ოპერაციების დისტანციური მონიტორინგი).



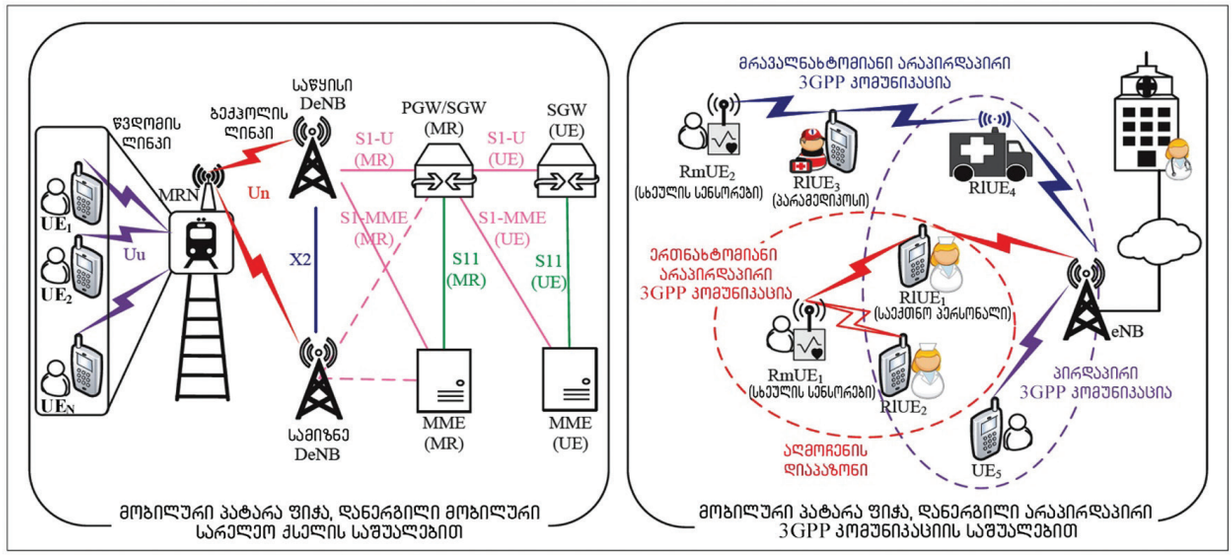
ნახ. 8.4. SECRET-ის საცდელი სტენდის არქიტექტურა (აკრონიმები მოცემულია წიგნის ბოლოს, განყოფილებაში: აბრევიატურები და აკრონიმები)

8.7. მობილური პატარა ფიჭების სტანდარტიზაცია

MSC პარადიგმის რეალიზაციამ ბოლო დროს მიიპყრო 3GPP-ის ყურადღება, სადაც შემოთავაზებულია სხვადასხვა ტექნოლოგია სტანდარტებში პოტენციური ჩართვისთვის. აღსანიშნავია, რომ მობილური სარელეო (MR) ტექნოლოგიების შესწავლა ჩატარდა გამოშვებებში R11 და R12. უფრო მეტიც, 3GPP სტანდარტი ასევე მოიცავს D2D-ის სიახლოვის სერვისებს (ProSe), რაც საშუალებას იძლევა განხორციელდეს ე. წ. 3GPP არაპირდაპირი კომუნიკაცია. ამ ტექნოლოგიების გამოყენება MSC-ების დანერგვისთვის შემდგომში სტანდარტების ევოლუციასთან ერთად განიხილება.

თავდაპირველად განკუთვნილი მაღალსიჩქარიანი მატარებლებისთვის, MR მიზნად ისახავს გააუმჯობესოს საბორტო UE-ების ფიჭური დაფარვა წვდომის მოწყობილობების, კერძოდ, მობილური სარელეო კვანძების (MRN) განლაგებით, რაც უზრუნველყოფს როგორც ბექჰოლის კავშირს eNB-ების მეშვეობით მანქანის მოძრაობის ტრაექტორიასთან ერთად, ასევე უსადენო დაკავშირებას UE-ებთან მანქანის შიგნით. კონცეფცია შეიძლება ადვილად გაფართოვდეს ტრანსპორტირების უფრო ზოგად ტიპებზე, რომლებსაც აქვთ მსგავსი სცენარის მახასიათებლები. კერძოდ, გადაადგილების ზომიერი და მაღალი სიჩქარე, უმეტეს შემთხვევაში ცნობილი (ან პროგნოზირებადი) ტრაექტორია, მაღალი შეღწევადობის დანაკარგები მანქანის სალონში და სტაციონარული ან ნახევრად სტაციონარული UE-ები მანქანის მოძრაობის მიმართულების მიხედვით.

MRN უსადენოდ არის დაკავშირებული დონორ eNB-სთან (DeNB) Un რადიოინტერფეისით, ხოლო საბორტო UE-ები უკავშირდებიან MRN-ს Uu ინტერფეისის მეშვეობით. MRN მხარს უჭერს UE ფუნქციების და eNB ფუნქციების ქვეჯგუფს, რათა დაუკავშირდეს DeNB-ს. SECRET-ის MSC-თან შესაბამისობაში, MRN-ები ასევე მხარს უჭერენ MRAT ფუნქციებს LTE Un-ის გამოყენებით ბექჰოლის ლინკში და რადიოინტერფეისის სხვადასხვა ტექნოლოგიების გამოყენებით (მაგალითად, LTE/3G/2G/WiFi) წვდომის ლინკში. როდესაც Un-ის ინტერფეისის კავშირი იცვლება სხვა DeNB-ზე ინტერ-DeNB HO-ის მეშვეობით, MRN-ებმა მაინც უნდა უზრუნველყონ უწყვეტი კავშირი საბორტო UE-ებთან ძირითადი ქსელის მიმართულებით. ზოგადად, MRN ტექნოლოგია არის შესაფერისი კანდიდატი MSC-ების ფუნქციონირების უზრუნველსაყოფად 3GPP B5G/6G ქსელებში. აღსანიშნავია, რომ ლიტერატურაში შემოთავაზებული იყო რამდენიმე MR არქიტექტურა და ჩატარებული შედარებითი კვლევის საფუძველზე შეირჩა ორი ვარიანტი MR-ებზე შემდგომი მუშაობისთვის. ნახ. 8.5 ასახავს ერთ ასეთ ვარიანტს, რომელშიც MR HO ხელახლა იყენებს არსებულ UE HO პროცედურებს გარკვეული ცვლილებებით.



ნახ. 8.5. *მარცხნივ: მობილური სარელეო არქიტექტურა, რომელიც მხარს უჭერს DeNB-ებს შორის ჰენდოვერს; მარჯვნივ: პატარა ფიჭების რეალიზაცია არაპირდაპირი 3GPP კომუნიკაციის საშუალებით (აკრონიმები მოცემულია წიგნის ბოლოს, განყოფილებაში: აბრევიატურები და აკრონიმები)*

R13-დან მოყოლებული, 3GPP სტანდარტმა შეიძლება მხარი დაუჭიროს MSC კონცეფციის განხორციელებას D2D ProSe-ის გამოყენებით, რაც დაუშვებს ორნახტომიან სარელეო ვარიანტს UE-სა და ქსელს შორის, არაპირდაპირი 3GPP კომუნიკაციით (i3Com). მიუხედავად იმისა, რომ თავდაპირველად ეს მიზნად ისახავდა მხოლოდ საავარიო-სამაშველო ოპერატორების მხარდაჭერას საზოგადოებრივი უსაფრ-

თხოების სიტუაციებში, დამატებითი სცენარები განისაზღვრა R16-ში (გამოყენება სახლებში, ჭკვიან ქარხნებში, ლოჯისტიკაში და ა. შ.).

I3Com უნდა იყოს მხარდაჭერილი დისტანციურ UE-სა (RmUE) და ქსელს შორის სარელეო UE-ის (RlUE) მეშვეობით, სადაც UE-ებს შორის კავშირს უნდა შეეძლოს E-UTRA-ის ან WLAN-ის გამოყენება. RlUE-ების მაქსიმალური რაოდენობა RmUE-სა და ქსელს შორის არის ერთი (ერთჯერადი ნახტომი) R16-ში, მაგრამ შეიძლება ეს მოთხოვნა შემსუბუქდეს R17-ში, რათა დაუშვას მრავალჯერადი ნახტომები. ქსელი იქნება პასუხისმგებელი UE-ის ავტორიზაციაზე, ჩართვასა და გამორთვაზე, რომ იმოქმედოს, როგორც RlUE. ქსელის მიერ RmUE-ის კონტროლი ასევე განხორციელდება i3Com-ის მეშვეობით WLAN-ის გამოყენებით. რამდენიმე RlUE შეიძლება ხელმისაწვდომი იყოს RmUE-ის სიახლოვეს და შესაბამისად, i3Com მხარს დაუჭერს RlUE-ის აღმოჩენას, შერჩევას და ხელახლა არჩევას სხვადასხვა კრიტერიუმის კომბინაციის საფუძველზე. ხელახალი არჩევა შეიძლება გამოწვეული იყოს შერჩევის კრიტერიუმების ნებისმიერი დინამიკური ცვლილებით, მათ შორის RlUE-ის ბატარეის ამოწურვით, ახალი სარელეო შესაძლებლობების მქონე UE-ის დიაპაზონში მოხვედრით, RmUE-ის სერვისის უფრო მაღალი ხარისხის მოთხოვნით და ა. შ. ზოგადად, i3Com-ის გამოყენებამ არ უნდა გამოიწვიოს ენერგიის მოხმარების გაზრდა RmUE-ზე, იმავე ტრაფიკისთვის, პირდაპირ 3GPP კომუნიკაციასთან შედარებით. ნახ. 8.5 (მარჯვნივ) ასახავს i3Com-ის კონცეფციას.

სარელეო ტექნოლოგიის ბოლოდროინდელმა აღორძინებამ, როგორც ჩანს, იმპულსი მოიპოვა 3GPP-ში ინტეგრირებული წვდომისა და ბექჰოლის (IAB) ტექნოლოგიის დანერგვით. IAB კვანძების განთავსება საშუალებას იძლევა, მოთხოვნის საფუძველზე მოხდეს სიხშირული სპექტრის გაერთიანება წვდომის ლინკსა და ბექჰოლის ლინკს შორის. მოსალოდნელია, რომ IAB კვანძების ამჟამინდელი სტაციონარული განმარტება მომავალ გამოშვებებში გადაიქცევა მობილურ IAB კონცეფციებად, რაც საშუალებას მისცემს MSC კონცეფციას, იყოს გამოყენებული. მომავალი 3GPP სტანდარტების კიდევ ერთი მოსალოდნელი მიმართულებაა მომხმარებელზე ორიენტირებული უფიჰო კავშირის მიდგომის პოპულარიზაცია, რომელიც უზრუნველყოფს ენერგოეფექტიანი მობილურობის მართვას. SECRET-ში შემოთავაზებული აპლინკის ზონდირების საცნობარო სიგნალის HO პროცედურა აჩვენებს გაუმჯობესებულ მახასიათებლებს HO-ის ოვერჰედის თვალსაზრისით SC-ების განთავსებისას. ამ კონცეფციის გაფართოება MSC-ებზე ან MRN-ებზე მოსალოდნელია, რომ მსგავს სარგებელს მოიტანს.

8.8. მერვე თავის დასკვნა

ეს თავი წარმოგვიდგენს SECRET მიდგომას B5G/6G ქსელების შესაქმნელად, რომელიც დაფუძნებულია ვირტუალურ მობილურ პატარა ფიჭებზე. ისინი აღიქმება ქსელის მიერ, როგორც ახალი ქსელური რესურსების აუზი, სადაც მემკვიდრეობით გადაცემულია 4C შესაძლებლობები და რომლის კონფიგურაციაც შეიძლება განისაზღვროს მოთხოვნისამებრ. ეს საშუალებას მოგვცემს დავნერგოთ 6G-სთან თავსებადი ახალი სერვისები, როგორიცაა მაგალითად, URLLC, ასევე მნიშვნელოვნად შემცირდეს შესაბამის ინფრასტრუქტურაზე დაფუძნებული განთავსების ღირებულება.

ამ მიზნით, განხილულ იქნა გამოწვევები, გაუმჯობესებული ტექნოლოგიები და გადაწყვეტილებები საცდელ სტენდთან ერთად, რომელიც აჩვენებს SECRET კონცეფციის სარგებლიანობას. დადგენილია, რომ SECRET არქიტექტურა, რომელიც იმართება განაწილებული SDN არქიტექტურით, უზრუნველყოფს უსაფრთხო, საიმედო და ეფექტიან კომუნიკაციებს, თანდაყოლილი შესაძლებლობებით მხარი დაუჭიროს დაბალი შეყოვნების და ღრუბლოვანი გამოთვლების მქონე 6G სერვისებს. ვფიქრობთ, ასეთი მიდგომის ევოლუცია სამომავლო სტანდარტებში იქნება გათვალისწინებული.

თავი 9. ზონდირების, კომუნიკაციების და უსაფრთხოების ინტეგრირება 6G ქსელებში

9.1. შესავალი

6G ქსელი, რომელიც არის არა მხოლოდ არსებული საკომუნიკაციო ტექნოლოგიების გაუმჯობესება ან გაფართოება, არამედ დიდი პარადიგმული რევოლუცია, განიხილება, როგორც მომავალი ინტელექტუალური სამყაროს ახალი მამოძრავებელი ძალა. გარდა კვანძების დაკავშირებისა, 6G მხარს დაუჭერს ყოვლისმომცველ ზონდირებას, კომუნიკაციას და ინტელექტს. 6G-ის საინტერესო მახასიათებლებს შორის, ზონდირება ანუ გამომჟღავნების ფუნქცია დამხმარე ფუნქციიდან ძირითად სერვისად გადაიქცევა, რაც ქსელის შესაძლებლობების დამატებით განზომილებას უზრუნველყოფს. ამან გამოიწვია ბოლოდროინდელი კვლევითი ინტერესი ISAC-ის მიმართ, როგორც ტექნოლოგიის, რომელიც იძლევა ზონდირებისა და საკომუნიკაციო ფუნქციების ინტეგრირების საშუალებას ერთი გადაცემით, ერთი მოწყობილობით და საბოლოოდ, ერთიანი ქსელის ინფრასტრუქტურით. საერთო სპექტრის, აპარატურული პლატფორმისა და სიგნალის დამუშავების სტრუქტურის გამოყენებით, ISAC-ს შეუძლია გააუმჯობესოს სპექტრული ეფექტიანობა და ენერგოეფექტიანობა, რითაც გადაჭრის სპექტრის გადატვირთულობის პრობლემას და ამავდროულად შეამცირებს ტექნიკური აღჭურვილობისა და სიგნალიზაციის ხარჯებს, რომელსაც ეწოდება ინტეგრაციის მოგება. გარდა ამისა, ორი ფუნქციის ერთობლივი დიზაინის შესაძლებლობის გამოყენებით, ISAC-ს შეუძლია უზრუნველყოს კომუნიკაციაზე დაფუძნებული ზონდირება და ზონდირებაზე დაფუძნებული კომუნიკაცია. აქედან გამომდინარე, მას შეუძლია მნიშვნელოვნად გააუმჯობესოს ზონდირებისა და კომუნიკაციის მახასიათებლები, რომელსაც კოორდინაციის მოგებას უწოდებენ. ზემოაღნიშნული უპირატესობების გამოყენებით, ISAC-ს შეუძლია ჩართოს ახალი აპლიკაციები, მათ შორის, გაუმჯობესებული ლოკალიზაცია და თვალთვალი, დრონის მონიტორინგი/მართვა, ადამიანის აქტივობის ამოცნობა, ავტომობილების ჯგუფის სინქრონული გადაადგილება, გარემოს მონიტორინგი, პროტოკოლები და ქსელურ დონეზე ზონდირება, სხივის ერთდროული სწავლება, თვალყურის დევნება და პროგნოზირება ზონდირების დახმარებით და მნიშვნელოვანი რესურსების (მაგალითად, ფიჭის HO-ის, სიხშირული ზოლის, ენერგეტიკული დანახარჯების და სხივის სიგანის) განაწილება.

მიუხედავად ამისა, ISAC-ის წინაშე დგას უსაფრთხოების უნიკალური გამოწვევები, რომლებიც წარმოიქმნება სპექტრის გაზიარების და უსადენო გადაცემის ბუნების გამო. საინფორმაციო შეტყობინებების ჩართვა სარადარო გამოკვლევის სიგნალში, კომუნიკაციას დაუცველს ხდის სამიზნის მოსმენის კუთხით. მართლაც, ზონდირებულ სამიზნეს შეუძლია, პოტენციურად გამოიყენოს ინფორმაციის შემცველი სიგნალი და მოახდინოს კონფიდენციალური შეტყობინების დეტექტირება, რომელიც განკუთვნილია საკომუნიკაციო მიზნებისთვის. ეს ქმნის უნიკალურ და ძალიან საინტერესო კომპრომისს გადამცემისთვის. ერთი მხრივ, მას სურს „გაანათოს“ სამიზნე, მისი მიმართულებით სიმძლავრის ფოკუსირებით, ხოლო მეორე მხრივ, უნდა შეზღუდოს სამიზნემდე მიმავალი სიგნალის სასარგებლო სიმძლავრე, რათა თავიდან აიცილოს მოსმენა.

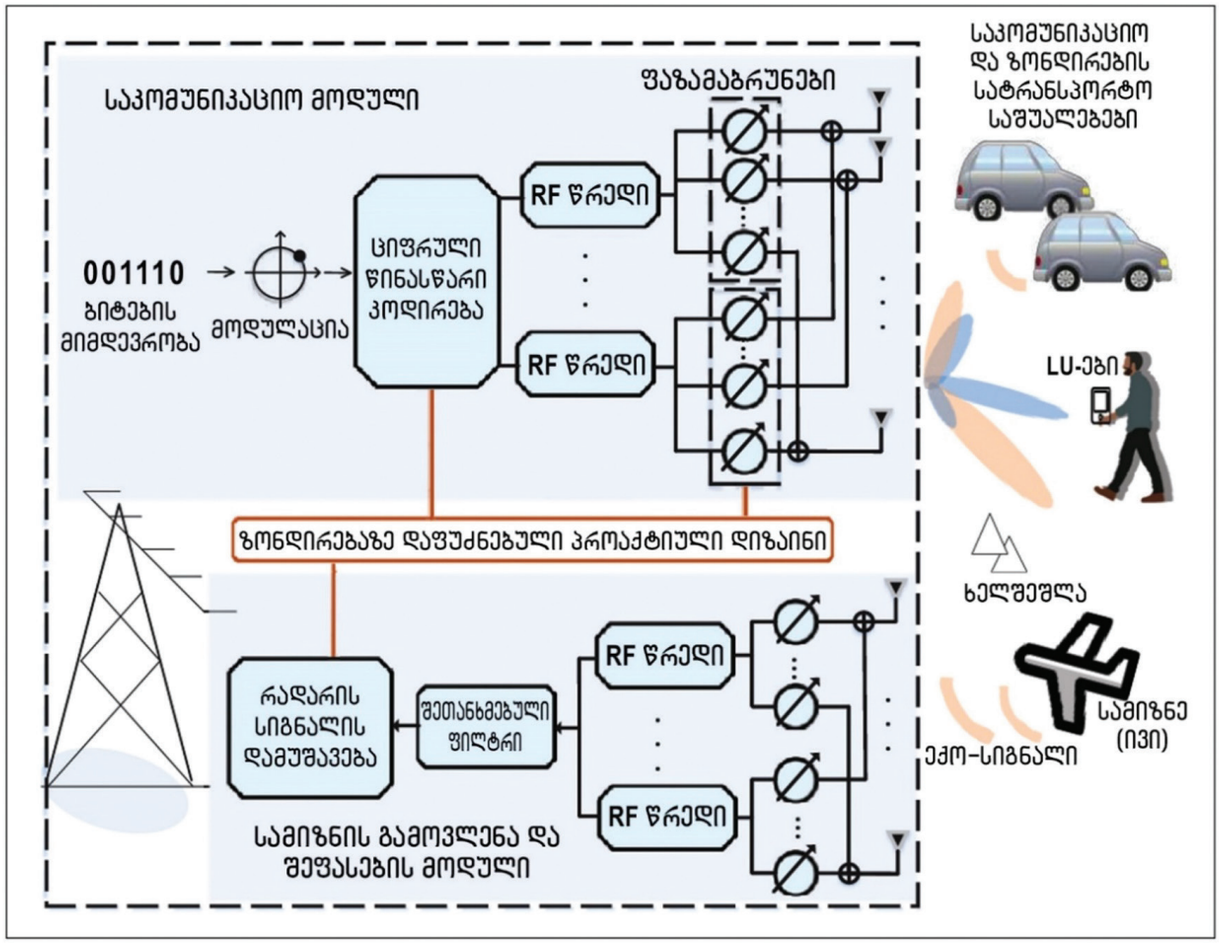
უსაფრთხოების ზემოაღნიშნული გამოწვევის შესაძლო გადაწყვეტა არის კრიპტოგრაფიული ტექნიკის გამოყენება ქსელის სტეკის ზედა ფენებში კონფიდენციალური მონაცემების დაშიფვრით გადაცემამდე. თუმცა, ასეთ გადაწყვეტილებებს აქვს რამდენიმე შეზღუდვა, როგორიცაა საიდუმლო გასაღების მართვის/მომსახურების დამღლელი პროცესი, უსაფრთხოების დაუდასტურებელი მახასიათებელი გამოთვლითი კუთხით ძლიერი მომსმენის ივის (Eve) თანდასწრებით და კომპრომეტირებული

საიდუმლო გასაღების იდენტიფიცირების სირთულე. ფიზიკური ფენის უსაფრთხოება, როგორც ინფორმაციის თეორიაზე დაფუძნებული მეთოდოლოგია, შეიძლება იყოს დამატებითი მიდგომა უსაფრთხო უსადენო გადაცემის უზრუნველსაყოფად. ივებსა და ლეგიტიმურ მომხმარებლებს შორის არხის ცვალებადობის გამოყენებით, სიგნალის ხარისხი, რომელსაც ივები იღებს, შეიძლება დაქვეითდეს იმ ხარისხამდე, რომ ივებმა ვერ შეძლონ შეტყობინების ამოღება მაშინაც კი, როდესაც მათ საიდუმლო გასაღების შესახებ სრული ცოდნა ექნებათ. მიუხედავად ათწლეულების კვლევისა, PHY უსაფრთხოების გადაწყვეტილებების დიდი კლასის ძირითადი შეზღუდვა გამომდინარეობს უკიდურესად ოპტიმისტური ან ზედმეტად პესიმისტური ვარაუდებიდან იმის შესახებ, თუ რა შეიძლება იყოს ცნობილი ივის შესახებ. ზოგიერთი მეთოდი მოითხოვს ივის არხების სრულ ცოდნას ან მათზე სტატისტიკურ ინფორმაციას; ზოგიერთი მეთოდი არ საჭიროებს რაიმე ცოდნას ივის არხების შესახებ, როგორიცაა ხელოვნური ხმაურის გადაცემა მთელი სივრცის დასაბლოკად, ლეგიტიმური დანიშნულების ადგილის გარდა. თუმცა, ასეთი მეთოდები არ უზრუნველყოფს ხელმისაწვდომი სიხშირის გატარების ზოლის ეფექტიან გამოყენებას ისეთი სიგნალის გადაცემის გამო, რომელიც არ შეიცავს საკომუნიკაციო ინფორმაციას. ახლახან ჩატარდა სამუშაოები, რომლებიც მონიტორინგს უწევს ივის რადიოსიხშირული ელექტრომაგნიტური ტალღების ველთან ურთიერთქმედებით გამოწვეულ ცვლილებებს PHY დონეზე, ივის პოზიციის დასადგენად. თუმცა, ზონდირება და კომუნიკაცია ცალ-ცალკე ხორციელდება და შესაბამისად, ივის მიერ მიღებული ინფორმაცია შეიძლება იყოს მოძველებული, განსაკუთრებით, მაღალი მობილურობის მქონე სცენარებში. ასევე, ეს მიდგომა არ არის სპექტრულად ეფექტიანი, რადგან სპექტრული რესურსები მხოლოდ ზონდირებისთვისაა გამოყენებული.

საინტერესოა, რომ ISAC-ის ერთობლივი ზონდირებისა და კომუნიკაციის მექანიზმი ხსნის ახალ შესაძლებლობებს უსაფრთხო დიზაინისთვის, სადაც ზონდირების დამატებითი ფუნქციები შეიძლება განხილული იყოს, როგორც მხარდაჭერა, უსაფრთხოების უზრუნველყოფის გასაადვილებლად. აღნიშნული საკითხით მოტივირებული ეს თავი მიმოიხილავს ზონდირებაზე დაფუძნებულ უსაფრთხო დიზაინებს ISAC-ის მახასიათებლებთან ერთად. ISAC სისტემების საფუძვლებიდან დაწყებული, ჩვენ პირველ რიგში, ახალ უსაფრთხო ISAC დიზაინს შევისწავლით, შემდეგ განვიხილავთ პრაქტიკულ, საიმედო უსაფრთხო ISAC დიზაინს, სადაც სამიზნის და კომუნიკაციის მომხმარებლების შესახებ ინფორმაცია არასრულყოფილად არის მოპოვებული. გარდა ამისა, განიხილება ზოგიერთი აპარატურის ეფექტიანი, უსაფრთხო ISAC არქიტექტურა. შემდეგ იდენტიფიცირებულია ღია გამოწვევები და მოცემულია დასკვნები.

9.2. ISAC-ის საფუძვლები

ISAC-ის განვითარების ადრეულ ეტაპზე, საკომუნიკაციო და სარადარო სპექტრის გაზიარება (CRSS) გამოკვლეული იყო სპექტრის ზონდირების, სპექტრის დინამიკური წვდომისა და ურთიერთინტერფერენციების თავიდან აცილების თვალსაზრისით ისე, რომ საკომუნიკაციო და სარადარო სისტემებს შეძლებოდათ სპექტრის გაზიარება ერთმანეთისთვის მნიშვნელოვანი ინტერფერენციების შექმნის გარეშე. როგორც შემდგომი ნაბიჯი, დადგინდა, რომ ISAC-ს შეუძლია უზრუნველყოს არა მხოლოდ სპექტრული თანაარსებობა, არამედ HW-ის პლატფორმისა და ქსელის არქიტექტურის საერთო გამოყენებაც, როგორც ნაჩვენებია ნახ. 9.1-ზე. გარდა საკომუნიკაციო და ზონდირების ფუნქციების უზრუნველყოფისა, ISAC სისტემები ემსახურება კომუნიკაციაზე დაფუძნებული ზონდირების და ზონდირებაზე დაფუძნებული კომუნიკაციის ფუნქციებს. დავიწყოთ ISAC-ის საფუძვლების განხილვით და შემდეგ გადავიდეთ უსაფრთხო ISAC გადაცემაზე.



ნახ. 9.1. კომუნიკაციისა და ზონდირების ერთობლივი დიზაინი ISAC-სთვის. გადამცემის მხარეს, მოდულირებული სიგნალი რეგულირებულია ციფრული წინასწარი კოდირებით საბაზისო ზოლში, შემდეგ გადის RF წრედებში და საბოლოოდ, ანტენებით იშლება. მეორე მხრივ, სანამ არეკლილი ექო-სიგნალი ანალიზდება სამიზნის აღმოჩენისთვის, ზონდირების შედეგები ასევე ხელს უწყობს უსაფრთხო ტალღის დიზაინს პროაქტიული და მიზეზობრივ-შედეგობრივი გზით

მაშინ, როდესაც კომუნიკაცია მიზნად ისახავს ინფორმაციის უშეცდომოდ გადაცემას მიმღებამდე, ზონდირების ამოცანაა სამიზნის ინფორმაციის ამოღება სამიზნის ექოდან. მაშასადამე, ზონდირებისთვის სასარგებლო ინფორმაცია მოთავსებულია არა მისი ტალღის ფორმაში, არამედ სამიზნიდან დაბრუნებულ სიგნალში. საინტერესოა აღინიშნოს, იმის გამო, რომ ზონდირების და კომუნიკაციის ეფექტიანობა ფასდება სხვადასხვა KPI-ებით, ISAC ტალღის ფორმის შემუშავებისას გათვალისწინებულ უნდა იქნეს სხვადასხვა მეტრიკა ორმაგი ფუნქციის განსახორციელებლად. ეს, როგორც წესი, იწვევს ურთიერთსაწინააღმდეგო დიზაინის მიზნებს ზონდირებასა და კომუნიკაციებს შორის, რომლებიც ყურადღებით უნდა იყოს დაბალანსებული, როგორც ეს დეტალურად არის აღწერილი ქვემოთ.

ISAC ტალღის ფორმის დიზაინი შეიძლება დაიყოს ზონდირებაზე ორიენტირებულ, კომუნიკაციაზე ორიენტირებულ და ერთობლივ დიზაინებად:

ზონდირებაზე ორიენტირებული დიზაინი: აღნიშნული დიზაინი აერთიანებს საკომუნიკაციო შეტყობინებებს კლასიკური ზონდირების ტალღურ ფორმაში და შესაბამისად, აქვს მაღალი თავსებადობა რადარის არქიტექტურასთან. ადრეული დიზაინის სამუშაოები მოიცავდა იმპულსის ინტერვალის მოდულაციას, სადაც რადარის იმპულსებს შორის ინტერვალი გამოიყენება კომუნიკაციისთვის. ასევე, არსებობს დიზაინები, რომლებიც იყენებენ ინდექს-მოდულაციას ან განზოგადებულ სივრცულ მოდულა-

ციას ტალღის ფორმის დიზაინისთვის. დიზაინის კიდევ ერთი მიდგომაა სამიზნის დადგენა რადარის სხივის მიმართულობის დიაგრამის მთავარ წილში, ხოლო ინფორმაციის ჩასმა – სხივის მიმართულობის დიაგრამის გვერდით წილებში. მიუხედავად ამისა, იმის გამო, რომ საკომუნიკაციო სიმბოლოები, როგორც წესი, ჩართულია რადარის იმპულსებში, ეს დიზაინი იწვევს მონაცემთა დაბალ სიჩქარეს, რომელიც შეზღუდულია რადარის იმპულსების გამეორების სიხშირით და რაც 5G/6G-სთვის დადგენილ მოთხოვნილებებზე ბევრად დაბალია.

კომუნიკაციაზე ორიენტირებული დიზაინი: კომუნიკაციაზე ორიენტირებული დიზაინი ზონდირებისთვის იყენებს სტანდარტიზებულ კომუნიკაციის ტალღის ფორმებს, პროტოკოლებსა და არქიტექტურებს. მაგალითად, პილოტ-სიგნალები და ფრეიმის პრეამბულები, რომლებსაც აქვთ კარგი ავტოკორელაციის თვისებები და როგორც წესი, გამოიყენება არხის შეფასებისთვის ან მრავალი მომხმარებლის წვდომისთვის, ახლახან გამოიყენეს სამიზნეების ზონდირებისთვის. ასევე, სტანდარტებთან შესაბამისი საკომუნიკაციო ტალღების ფორმები, გამოყენებული იქნა სამიზნეების ზონდირებისთვის სატრანსპორტო პროგრამებში. ამ კომუნიკაციაზე ორიენტირებულ ISAC დიზაინებს შეუძლიათ განახორციელონ ზონდირების ფუნქციები საკომუნიკაციო მახასიათებლების გაუარესების გარეშე, რითაც უზრუნველყოფენ მონაცემთა გადაცემის მაღალ სიჩქარეს. თუმცა, პილოტ-სიგნალი, ფრეიმის პრეამბულები და საკომუნიკაციო ტალღის ფორმები არ არის სპეციალურად ზონდირებისთვის შექმნილი. შესაბამისად, კომუნიკაციაზე ორიენტირებული დიზაინის მთავარი ნაკლია ცუდი, სცენარზე დამოკიდებული და ძნელად დასარეგულირებელი ზონდირების მახასიათებლები.

ერთობლივი დიზაინი: ერთობლივი დიზაინის ISAC მიდგომებში, სხივის მიმართულობის დიაგრამა შექმნილია ისე, რომ შეესაბამებოდეს რადარის იდეალურ სხივს და ამავე დროს, უზრუნველყოს სიგნალის ინტერფერენცია-პლუს-ხმაურთან მაღალი თანაფარდობა (SINR) LU-ებში ეფექტიანი კომუნიკაციების განსახორციელებლად. ჯამურად შეწონილი ზონდირებისა და კომუნიკაციის ხარისხი ასევე შეიძლება იქნეს გამოყენებული, როგორც მიზნობრივი ფუნქცია, რაც შემდგომში მიგვიყვანს პარეტოს განაწილების ოპტიმალურობაზე დაფუძნებულ მრავალმიზნობრივ ოპტიმიზაციამდე. გარდა ოპტიმიზაციაზე ორიენტირებული კვლევისა, ერთობლივი დიზაინი ასევე, გამოკვლეულ იქნა ინფორმაციის თეორიის პერსპექტივიდან, როგორიცაა არხის კოდირების შემუშავება, ისევე როგორც თეორიული ურთიერთდამოკიდებულება გადაცემის სიჩქარესა და ზონდირების მახასიათებლის დიზაინს შორის. ცხადია, რომ ერთობლივი დიზაინი მოიცავს ორივე ფუნქციის სათანადო ოპტიმიზაციას და უზრუნველყოფს მათ შორის შესრულების მასშტაბირებად კომპრომისებს. ის იძლევა დროითი, სიხშირული და სივრცითი რესურსების მოქნილ გამოყენებას, რითაც მიიღწევა როგორც მაღალი გამტარუნარიანობა, ასევე ზონდირების საიმედოობა. გარდა აკადემიური კვლევებისა, განხორციელდა ფართო ინდუსტრიული საქმიანობა, რომელიც ფოკუსირებულია ISAC-ზე, მათ შორის 3GPP-ის კუთხით (მაგალითად, S1-214036/214056/214100/214101, R1-2110894/2104724, და R2-210049), ასევე შემუშავდა ელექტრო და ელექტრონიკის ინჟინრების ინსტიტუტის (IEEE) სტანდარტები (მაგალითად, 802.11bf, 802.15.22.3-2020 და 802.11-2020) და ITU-ის რეკომენდაციები (მაგალითად, ITU-T Y.4809 და ITU-T X.1080.2).

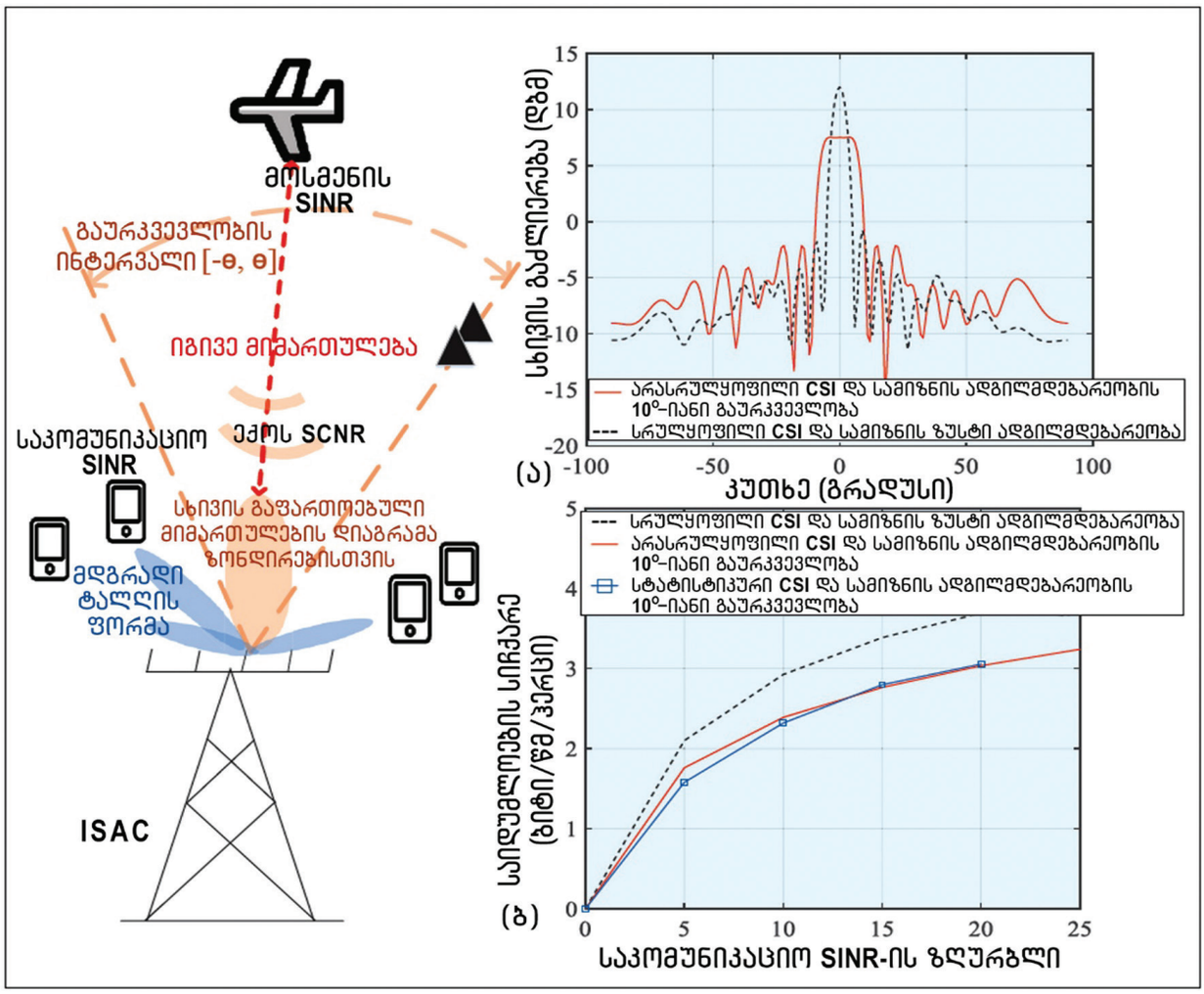
9.3. უსაფრთხოების ინტეგრირება ISAC-ში

ამ პარაგრაფში ჩვენ შევისწავლით ISAC-თან დაკავშირებულ უსაფრთხოების საკითხებს და დავადგენთ, თუ როგორ შეიძლება ზონდირების ფუნქცია გონივრულად იქნეს გამოყენებული ინფორმაციული უსაფრთხოების უზრუნველყოფის მიზნით.

ISAC-ის გადამცემს სჭირდება თავისი სიმძლავრის ფოკუსირება სამიზნეების შემცველ მიმართულებებზე და იმის უზრუნველყოფა, რომ მიმღებზე სამიზნის ექოს აქვს საკმარისად კარგი სიგნალის

ხელშეშლა-პლუს-ხმაურთან თანაფარდობა (SCNR) ზონდირების გარკვეული მახასიათებლების მისაღწევად. თუმცა, რამდენადაც სამიზნე შეიძლება იყოს ივი, ზონდირების სხივის კუთხე, რომელიც შედის SCNR-ის ობიექტივში, იგივეა, რაც ივის კუთხე, როგორც ნაჩვენებია ნახ. 9.2-ზე. ეს გულისხმობს, რომ სამიზნეს აქვს მაღალი მიღებული SINR ჩაშენებულ საკომუნიკაციო სიგნალზე, რაც საგრძნობლად ზრდის სამიზნის მიერ ინფორმაციის მოსმენისადმი მგრძნობელობას. ამიტომ, ფრთხილად უნდა მოხდეს კომპრომისი სამიზნის მიმართულებით ზონდირებისთვის საკმარისი სიმძლავრის გაგზავნას და სამიზნეზე სასარგებლო სიგნალის სიმძლავრის შეზღუდვას შორის, მოსმენის თავიდან ასაცილებლად. ქვემოთ განვიხილავთ უახლესი კვლევის შედეგებს ზონდირების გამოყენებით უსაფრთხო ISAC მეთოდების შემუშავების შესახებ.

ISAC გადამცემს შეუძლია სამიზნიდან არეკლილი ექო-სიგნალის ტალღის მოსვლის კუთხის (AoA) ზონდირება და მიღებული სიგნალის სიმძლავრის მიხედვით სამიზნის პოზიციის განსაზღვრა. ამ ორმხრივი არხის გამოყენებით შეიძლება შეფასდეს მოსმენის არხი ISAC გადამცემიდან სამიზნემდე. აქედან გამომდინარე, პროაქტიულად და შემთხვევით მიღებული მოსმენის არხი ან სამიზნის AoA, როგორც მინიმუმ, შეიძლება გამოყენებულ იქნეს მრავალი უსაფრთხო მიდგომის შესაქმნელად, რომელთა შორისაა: უსაფრთხო სხივის ფორმირება, ხელოვნური ხმაური, ერთობლივი ჩახშობა და ა. შ.



ნახ. 9.2. პრაქტიკული სცენარი, სადაც ხდება სამიზნის პოზიციის უხეში ზონდირება გაურკვევლობის ინტერვალში და LU-ის არხები ასევე არასრულყოფილად არის ცნობილი: ა) სხივის მიმართულობის დიაგრამის სიგანე ადაპტიურად რეგულირდება სხვადასხვა სცენარში სამიზნის ზონდირებისთვის; ბ) სამიზნის პროაქტიული ზონდირებით მიიღწევა საიდუმლოების სიჩქარის მაღალი დონე

ISAC-ის უნიკალური გადაცემა მოითხოვს ზემოაღნიშნული მიდგომების ხელახალ დიზაინს, რათა მიაღწიოს ორმაგ ფუნქციონალურობას „შიდა ზოლში“. მაგალითად, უსაფრთხო ორმაგი ფუნქციონალური გადაცემის შემუშავებისას, შესაძლებელია ზონდირების მახასიათებლების ოპტიმიზაცია ISAC-ის მიმღებზე ექო-სიგნალის SCNR-ის მაქსიმალურად გაზრდით, სამიზნეზე მოსმენის SINR-ის შეზღუდვით და ამავე დროს, LU-ებზე სიგნალის SINR-ის გარანტირებული მნიშვნელობით გარკვეულ ზღურბლს ზემოთ. ეს ეკვივალენტურად აუმჯობესებს „საიდუმლოების სიჩქარის“ მნიშვნელობას, რომელიც ზოგადად განისაზღვრება, როგორც სხვაობა ძირითადი საკომუნიკაციო არხის სიჩქარესა და მოსმენის მაქსიმალურ სიჩქარეს შორის. ჩვენს შემთხვევაში იგი წარმოადგენს მიღწევადი სიჩქარეების სხვაობას LU-ებსა და სამიზნეს შორის. ალტერნატიულად, შეგვიძლია მაქსიმალურად გავზარდოთ საიდუმლოების სიჩქარე და იმავდროულად, უზრუნველვყოთ ეხოს SCNR ISAC-ის მიმღებზე რადარის გარანტირებული ფუნქციონირებისთვის. მიუხედავად იმისა, რომ ზონდირებით შემუშავებული უსაფრთხო ტალღის ფორმა არ არის ბუნებრივად ამოზნექილი, ზონდირების და საკომუნიკაციო ფუნქციების ფრაქციულად სტრუქტურირებული SINR და SCNR შეზღუდვების გამო, არსებობდა ოპტიმიზაციის ფართო შესაძლებლობები ISAC სისტემებში ამ ტიპური ფრაქციული სტრუქტურირებული ოპტიმიზაციის განსახორციელებლად. გასათვალისწინებელია ის გარემოებაც, რომ იმ იშვიათ შემთხვევაში, როდესაც სამიზნე და LU არის ერთი და იგივე მიმართულებით და ორივეს აქვს ძლიერი პირდაპირი ხედვის ხაზის (LoS) არხები, ისინი მჭიდრო კორელაციაშია. ამ კონტექსტში, PHY ფენაზე უსაფრთხოების უზრუნველყოფა უკიდურესად რთულია, სადაც უსაფრთხო ავთენტიფიკაციისა და დაშიფვრის მეთოდების გამოყენება ჯერ კიდევ აუცილებელია მაღალ ფენებში.

პრაქტიკაში, სამიზნის პოზიცია ყოველთვის სრულყოფილად არ არის განსაზღვრული ზონდირების შეცდომისა და გამოვლენის სასრული გარჩევადობის გამო. მაგალითად, თუ გვაქვს N ანტენა, რომელიც განლაგებულია ერთგვაროვან წრფივ სტრუქტურაში, ტალღის სიგრძის ნახევრის დაშორებით, კუთხის გარჩევადობა დაახლოებით გამოითვლება, როგორც 2/N (რადიანებში), რაც ნიშნავს, რომ ამ კუთხური ინტერვალის ფარგლებში სამიზნეების ინდივიდუალურად გამოვლენა შეუძლებელია. როდესაც სამიზნის პოზიციის უხეშად დადგენა შესაძლებელია მხოლოდ კუთხოვანი რეგიონის ფარგლებში, საჭიროა უფრო ფართო სხივის ჩამოყალიბება ამ რეგიონის მიმართულებით, რათა არ გამოვტოვოთ სამიზნე. თუმცა, სხივის ფოკუსირება სივრცის რეგიონში აუცილებლად იწვევს ინფორმაციის გაჟონვის შესაძლებლობას, რაც წარმოშობს ტალღის ფორმის საიმედო და უსაფრთხო დიზაინის საჭიროებას.

როდესაც ცნობილია, რომ სამიზნე მდებარეობს მხოლოდ სივრცის გარკვეულ კუთხოვან რეგიონში, საიმედო უსაფრთხო ტალღის ფორმა შეიძლება მიღებულ იქნეს სამიზნის მიღების SINR ჯამის მინიმიზაციის გზით, ამ კუთხური ინტერვალის შესაძლო მდებარეობებზე. ამ გზით, სამიზნის მიღწევადი საიდუმლოების სიჩქარე შეიძლება იყოს ზემოდან შემოსაზღვრული, რაც ინფორმაციის უსაფრთხოებას უზრუნველყოფს. მეორე მხრივ, როდესაც LU-ების არხები ასევე არ არის სრულყოფილად ცნობილი ISAC გადამცემისთვის, არხის შეფასების შეცდომა შეიძლება ზოგადად ჩამოყალიბდეს შემოსაზღვრული ან შემოუსაზღვრავი შეცდომის მოდელების გამოყენებით. აღნიშნული შეცდომის მოდელებით შესაძლებელია იმის უზრუნველყოფა, რომ LU-ების SINR შეიძლება შემდგომ გარდაიქმნას დეტერმინისტულ ან ალბათურ შეზღუდვებად, რომლებიც ადვილად შეიძლება დამუშავდეს დადგენილი სტოქასტური ოპტიმიზაციის მეთოდების მეშვეობით.

განვიხილოთ ნახ 9.2-ზე ნაჩვენები სცენარი, სადაც სამიზნის შესაძლო კუთხური ინტერვალი არის [–5°, 5°], ხოლო LU-ების არხის შეფასების შეცდომა შეესაბამება გაუსის განაწილებას დისპერსიით 0.05. გამოყენებულია 4 LU და მათი SINR-ის ზღურბლი არის 40 დბ. ენერგიის ბიუჯეტი არის 20 დბმ. უსაფრთხო ტალღის ფორმის ოპტიმიზაციის მიზანია სამიზნის მიღების SINR-ის ჩახშობა SINR მოთხოვნების შესაბამისად თითოეული LU-სთვის; ამასთან, უზრუნველყოფილი უნდა იყოს მიღებული ტალღის ფო-

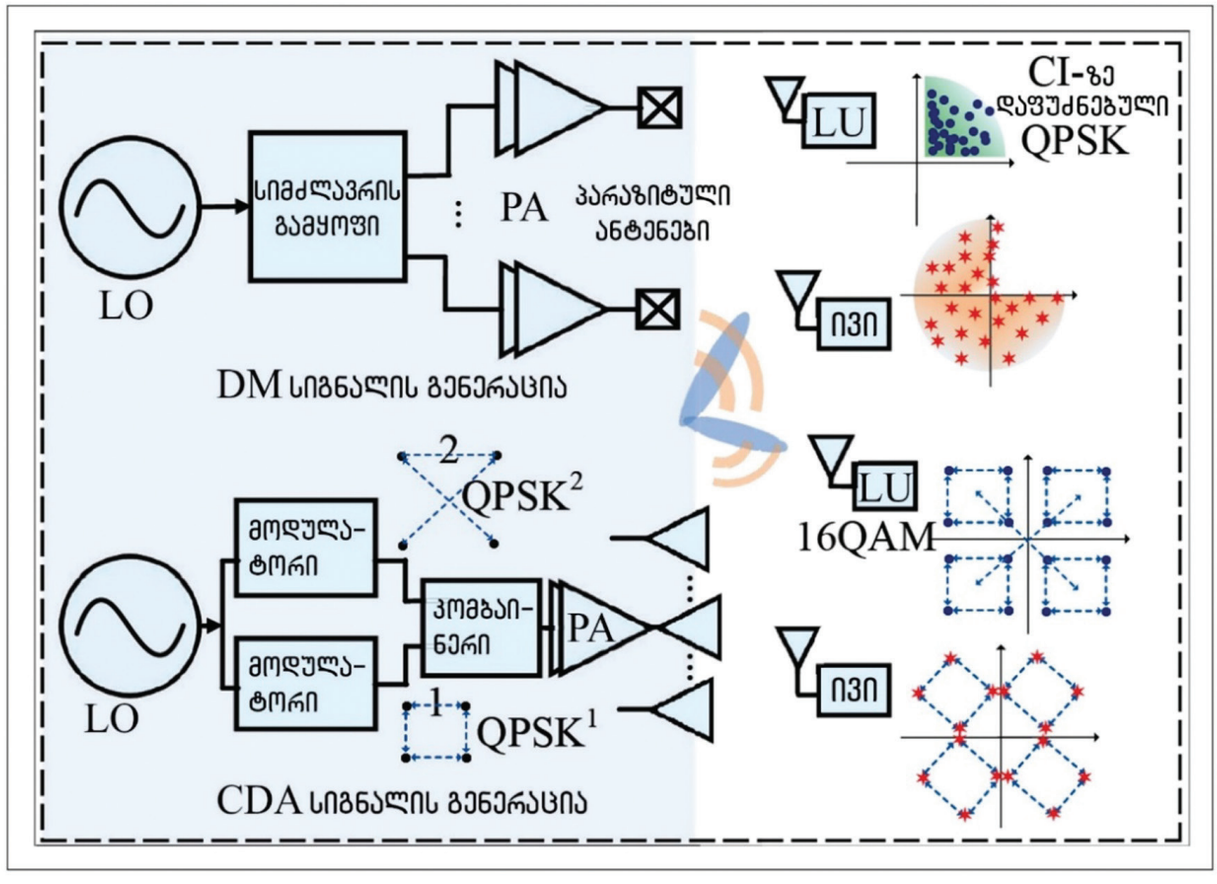
რმის მიახლოება ზონდირებისთვის სხივის სასურველ მიმართულობის დიაგრამასთან. როგორც ნახ. 9.2ა-დან ჩანს, სხივის ვიწრო მიმართულობის დიაგრამა მიიღება, როდესაც სამიზნის ადგილმდებარეობა ზუსტად არის ზონდირებული. პროაქტიულად მიღებული ადგილმდებარეობის გამოყენებით, გადამცემს შეუძლია მოახდინოს გაფანტული ტალღის ფორმის რეგულირება, რათა დათრგუნოს სამიზნის მოსმენის SINR, რითაც გააუმჯობესებს საიდუმლოების სიჩქარის დონეს (ნახ. 9.2ბ). როდესაც სამიზნის მდებარეობის მხოლოდ არასრულყოფილად ზონდირება შეიძლება, იქმნება სხივის უფრო ფართო მიმართულობის დიაგრამა, რომელიც მიმართავს იმავე სიმძლავრეს შესაძლო რეგიონზე, სხივის მთავარი წილის სიმძლავრის გაძლიერების შემცირებით. მიუხედავად ამისა, კუთხური ინტერვალის შესაძლო ადგილმდებარეობებზე სამიზნის SINR-ების ჯამის ჩახშობით, საიდუმლოების მაღალი სიჩქარე მიიღწევა მაშინაც კი, თუ ISAC გადამცემმა იცის მხოლოდ LU-ების არხების სტატისტიკა.

მილიმეტრული ტალღების დიაპაზონში, რომელიც კანდიდატი სიხშირეა 5G/6G სისტემებისთვის, სასურველია იაფი და ენერგოტევადი HW. თუმცა, აპარატურულმა შეზღუდვებმა შეიძლება საფრთხე შეუქმნას ზონდირების და კომუნიკაციის ფუნქციონირებას, რაც მთავარია, გადაცემის უსაფრთხოებას. თანამედროვე, აპარატურულად ეფექტიანი მოწყობილობების სიმრავლე, რომელიც შემუშავებულია მხოლოდ საკომუნიკაციო სისტემებისთვის, შეიძლება გამოყენებულ იქნეს „აპარატურულად ინფორმირებული“ უსაფრთხო ISAC გადაცემის შესაქმნელად. მაღალი აპარატურული ეფექტიანობით უსაფრთხო ტალღის ფორმირების ერთ-ერთი მიდგომაა RF წრედების შემცირება ანალოგური არქიტექტურის საშუალებით, რომელიც მოიცავს ფაზამაბრუნებს (PS) და/ან გადამრთველებს, როგორც ილუსტრირებულია ნახ. 9.1-ზე. ეს ჰიბრიდული ISAC მოიცავს დაბალგანზომილებიანი ციფრული სხივის ფორმირებას და მაღალგანზომილებიანი ანალოგური სხივის ფორმირებას. თუმცა, როგორც სრულად ციფრულ, ასევე ჰიბრიდულ ISAC-ში, RF წრედების საჭირო რაოდენობა არ არის ნაკლები, ვიდრე მონაცემთა ნაკადების საერთო რაოდენობა მრავალმომხმარებლიანი კომუნიკაციებისთვის.

ძვირად ღირებული და ენერგოტევადი ციფრულ-ანალოგური გარდამქმნელის (DAC) არგამოყენების მიზნით, ჩნდება HW-ის კუთხით უფრო ეფექტიანი უსაფრთხო ISAC აპარატურა, რომელიც აგებულია მიმართულებითი მოდულაციის კონცეფციაზე (DM), სადაც პარაზიტული ანტენები (ანუ პარაზიტული ელემენტების შემცველი ანტენები) გამოიყენება, როგორც ძირითადი კომპონენტები გადამცემში. LU-ების CSI-ის დახმარებით, სიმბოლოს მოდულაცია ხდება ანტენის დონეზე, ნაცვლად საბაზისო ზოლის დონისა, ხოლო მიღებული სხივის მიმართულობის დიაგრამა LU-ებში განიხილება, როგორც სივრცითი კომპლექსური სიგნალური კონსტელაციის წერტილი. კერძოდ, LU-ების მიერ კონსტრუირებული სიგნალი აუცილებლად არ ემთხვევა სასურველ სიმბოლოებს, მაგრამ შეიძლება დაშორდეს დემოდულაციისას დეტექტირების ზღურბლებს, რომლებიც აგებულია კონსტრუქციული ინტერფერენციის (CI) რეგიონების კონცეფციაზე.

მაგალითი ილუსტრირებულია ნახ. 9.3-ზე კვადრატული ფაზური მოდულაციისთვის (QPSK). ვინაიდან QPSK-სთვის გადაწყვეტილების ზღურბლები არის რეალური და წარმოსახვითი ღერძები, კონსტრუირებული სიმბოლოები (აღნიშნული ცისფერი წერტილებით) LU-ებში შეიძლება გონივრულად იქნეს გადატანილი როგორც რეალური, ისე წარმოსახვითი ღერძებიდან, სადაც რეზულტირებული გაზრდილი მანძილი დეტექტირების ზღურბლთან მიმართებაში სარგებლობის მომტანია LU-ების კომუნიკაციის ხარისხისთვის. ანალოგიურად, სიმბოლოები შეიძლება აგებულ იქნეს LU-ებისთვის უფრო მაღალი რიგის მოდულაციებით. მეორე მხრივ, პროაქტიულად მოპოვებული ივის ინფორმაციით, შეიძლება განზრახ განთავსდეს ივის მიერ მიღებული სიმბოლოები (აღნიშნული წითელი ვარსკვლავებით) სიგნალის დემოდულაციის დესტრუქციულ რეგიონებში, რაც კიდევ უფრო ართულებს ივისთვის „დაჭერის“ შესაძლებლობას სიმბოლოების დონეზე.

სხვა, ტექნიკური თვალსაზრისით ეფექტიან არქიტექტურას, კერძოდ, კონსტელაციის დაშლის მასივის (CDA) გამოყენებას, ასევე აქვს მაღალი პოტენციალი ISAC-ის დასაცავად. CDA-ის გამარტივებული ბლოკი ნაჩვენებია ნახ. 9.3-ზე, სადაც წარმოდგენილია ადგილობრივი ოსცილატორები (LO), მოდულატორები, წრფივი კომბაინერები და PA-ები, მაგრამ ძვირად ღირებული DAC-ები სრულიად გამორიცხულია. ცხადია, რომ მაღალი რიგის კვადრატული ამპლიტუდური მოდულაცია (QAM) შეიძლება განიხილებოდეს, როგორც რამდენიმე დაბალი რიგის QAM/QPSK სიგნალების ვექტორული კომბინაცია. მაგალითად, 16-QAM სიგნალი შეიძლება ჩაითვალოს $QPSK^1$ და $QPSK^2$ სიგნალების ერთობლიობად, სადაც ზედა ინდექსი აღნიშნავს ნორმალიზებულ ევკლიდურ მანძილს ორ მიმდებარე სიმბოლოს (სიგნალს) შორის. LU-ების CSI მნიშვნელობებით მასივის სათანადო კონტროლით, LU-ს შეუძლია დაინახოს განკუთვნილი სიგნალის სწორი კომბინაცია, ხოლო ნებისმიერი ივი (მათ შორის, ზონდირების სამიზნე), რომელიც მდებარეობს სხვა კუთხით, დემოდულაციისას მიიღებს დამახინჯებულ სიგნალს. ასევე, იმის გამო, რომ CDA გადასცემს დაბალი რიგის მოდულაციის სიგნალებს პიკური სიმძლავრის საშუალო სიმძლავრესთან თანაფარდობის დაბალი დონით, PA-ებისთვის წრფივობის მკაცრი მოთხოვნა სათანადოდ შესუსტებულია.



ნახ. 9.3. როგორც ძირითად კომპონენტებს DM იყენებს PA-ებს და პარაზიტულ ანტენებს, ხოლო CDA იყენებს მოდულატორებს, წრფივ კომბაინერებს და PA-ებს

9.4. ღია გამოწვევები და მომავალი სამუშაო

ISAC-ის შესაბამისი დიზაინი ჯერ კიდევ ღიაა და დარჩენილი პრობლემების გადაჭრა შესაძლოა საკომუნიკაციო ლიტერატურის გამოყენებით. ISAC დიზაინის ევოლუციის გზაზე CRSS სისტემას ჯერ კიდევ აქვს თავისი ბაზარი. შექმნილი ორმხრივი ინტერფერენციის გასაკონტროლებლად, არსებობს პა-

რამეტრები, რომლებიც გარდაიქმნება ერთ სისტემაში და ამავე დროს, შეიცავს იმპლიციტურ ინფორმაციას მეორეზე. ეს იწვევს კონფიდენციალურობის პრობლემას ორი სისტემისთვის და განსაკუთრებით, სამხედრო რადარებისთვის. ბოლოდროინდელმა კვლევებმა გამოავლინა მანქანურ სწავლებაზე დაფუძნებული რამდენიმე სქემა, რომელიც იყენებს წინასწარი კოდირების მოწყობილობაში არსებულ ინფორმაციას რადარის ადგილმდებარეობის დასადგენად. შედეგად, ღია პრობლემად რჩება რადარებსა და საკომუნიკაციო მოწყობილობებს შორის პარამეტრების გაცვლა ერთმანეთის კონფიდენციალურობის დაკარგვის გარეშე და ურთიერთინტერფერენციების მინიმალური დონის შენარჩუნებით.

ბოლო წლებში, 5G/6G აპლიკაციები ფოკუსირებულია ულტრა საიმედო, დაბალი შეყოვნების, მასობრივ D2D კომუნიკაციებზე. ეს აპლიკაციები მოიცავს ახალ მეტრიკასა და პროტოკოლებს, მათ შორის შეყოვნებას, საიმედოობას, უნებართვო მასობრივ წვდომას, მოკლე პაკეტებს და ა. შ. ISAC-ის უსაფრთხო მეთოდების გადახედვა ამ მკაცრი მოთხოვნების დასაკმაყოფილებლად და სირთულის და ოვერჰედის დაბალი მნიშვნელობების შესანარჩუნებლად არის კვლევების ნაყოფიერი სფერო. 5G სისტემებმა შემოიტანა ტალღების ფორმირების სტანდარტიზებული სერია, რომელთა შორისაა: ფილტრირებული OFDM, ფურიეს დისკრეტული გარდაქმნით განვრცობილი OFDM და ზოლოვანი ფილტრების ჯგუფზე დაფუძნებული მრავალგადამტანიანი QAM. ასევე, 5G-მ შემოგვთავაზა ადაპტიური უსადენო ინტერფეისის კონფიგურაცია, როგორიცაა ცვალებადი ფრეიმის სტრუქტურა და გადამტან სიხშირეებს შორის ადაპტიური ინტერვალი 15–120 კჰც-ის ფარგლებში. იბადება კითხვა, თუ როგორ გამოვიყენოთ ტალღის ფორმის მოქნილი სპეციფიკაცია და უსადენო ინტერფეისის კონფიგურაცია სხვადასხვა საკომუნიკაციო გარემოში და მახასიათებლების მიმართ სპეციფიკური მოთხოვნებით. აუცილებელი სამუშაოა ჩასატარებელი თეორიასა და პრაქტიკას შორის წარმოქმნილი უფსკრულის გადასალახად. ქსელის დიზაინი გამოკვლეულია ფიჭური საკომუნიკაციო სისტემებისთვის, სადაც დაფარვის ალბათობა და ერგოდიული გამტარუნარიანობა გაანალიზებულია სისტემატური გზით. ეს კვლევა ქსელის დონეზე იძლევა რეკომენდაციებს ქსელის დაგეგმვისა და საინჟინრო დიზაინის შესახებ, მთელი სისტემის ინტერესების გათვალისწინებით. მიუხედავად იმისა, რომ ISAC-თან დაკავშირებული არსებული კვლევები შესწავლილია მარტივ სცენარებში, მომავალ საკომუნიკაციო სისტემებში კვანძების ჰეტეროგენულობისა და მაღალი სიმკვრივის მხედველობაში მიღებით, ISAC-ის სისტემატური დიზაინი უფრო ფუნდამენტურ კვლევას მოითხოვს. მონაცემთა კონფიდენციალურობის გარდა, უსაფრთხოების კონცეფცია მნიშვნელოვნად განზოგადდა 5G/6G კომუნიკაციებში, როგორიცაა ფარულობა და კონფიდენციალურობა. ზოგიერთ სცენარში მომხმარებლებს სურთ სხვებთან კომუნიკაცია ფარულად, რომელსაც უწოდებენ გამოვლენის დაბალი ალბათობით კომუნიკაციას. ზონდირებასთან კოორდინირებულად, უფრო ადვილი ხდება შემოჭრილი მოწინააღმდეგის ინფორმაციის აღმოჩენა, რომელიც შემდეგ გამოიყენება ფარული ტალღის შესაქმნელად, მიმდინარე კომუნიკაციის დასამალად. მეორე მხრივ, ზონდირება შეიძლება მოწინააღმდეგემ გამოიყენოს მომხმარებელთა კონფიდენციალურობის დარღვევისთვის, როგორიცაა ფეხით მოსიარულეთა პოზიციებისა და ტრაექტორიების დადგენა, ასევე მომხმარებლების შენობების შიდა აქტივობების ვიზუალიზაცია. აქედან გამომდინარე, მოთხოვნადია ISAC-ის როლის გადახედვა უსაფრთხოების ახალი მახასიათებლების თვალსაზრისით.

9.5. მეცხრე თავის დასკვნა

არსებითად, ISAC-ს შეუძლია მოიპოვოს ორი მთავარი უპირატესობა ზონდირების და საკომუნიკაციო ფუნქციებთან შედარებით: ინტეგრაციის და კოორდინაციის მოგება. ამ ორი უპირატესობით, ISAC-ის გამოყენება გავრცელდება მრავალ ახალ სფეროზე, მათ შორის, 6G ქსელებზე. ეს თავი განიხილავს

ISAC-ისა და უსაფრთხოების საინტერესო კვეთას. ISAC-ის საფუძვლებიდან დაწყებული, თავდაპირველად ჩვენ წარმოვადგინეთ ტალღის ფორმის დიზაინის მეთოდოლოგია ერთობლივი ზონდირებისა და კომუნიკაციისთვის; შემდეგ განვიხილეთ ზონდირებაზე დაფუძნებული უსაფრთხო ISAC ტექნოლოგია, რომელმაც თავიდან უნდა აგვაცილოს ზონდირებისთვის განკუთვნილი ტალღის ფორმაში ჩადებული კონფიდენციალური სიგნალის მოსმენა სამიზნის მიერ. დაბოლოს, განხილულია ბოლოდროინდელი ინტერესი საიმედო და HW-ის კუთხით ეფექტიანი უსაფრთხო ISAC-ის მიმართ. ISAC დიზაინის წარმოდგენილი ოჯახი გთავაზობს ინფორმაციული უსაფრთხოების შენარჩუნების ფართო სფეროს პროაქტიული გზით, რაც მომავალ წლებში საინტერესო კვლევებს გვპირდება.

ბოლოთქმა

6G არის მობილური კომუნიკაციების მეექვსე თაობის სტანდარტი, რომელიც ამჟამად მუშავდება 5G-ის ჩანაცვლებისთვის. 6G გვთავაზობს სრულად ავტონომიური ქსელების ამბიციურ ხედვას, რომელიც კომერციულად განთავსდება 2030-იან წლებში. მკვლევრები იმედოვნებენ, რომ ეს სტანდარტი გააფართოებს კავშირებს, დაფარვისა და ქსელური შესაძლებლობებით უზრუნველყოფს ციფრული სერვისების ფართო სპექტრს, როგორიცაა: ტარებადი დისპლეები, იმპლანტირებული მოწყობილობები, ტელედასწრების აპლიკაციები (შეხვედრის თითოეული მონაწილის 3D ჰოლოგრაფიული წარმოდგენა), შერეული რეალობა, ტაქტილური და ინდუსტრიული ინტერნეტი და ავტონომიური მართვა. დაფარვისა და ქსელის ჰეტეროგენულობის მნიშვნელოვანი ზრდით, არსებობს სერიოზული შეშფოთების საფუძველი, რომ 6G უსაფრთხოება და კონფიდენციალურობა შეიძლება იყოს უარესი, ვიდრე წინა თაობებისთვის. დაკავშირებული მოწყობილობების ჩართვა ადამიანის ცხოვრების ყველა ასპექტში (მაგალითად, იმპლანტებისა და კიბორგების) სერიოზულ შეშფოთებას იწვევს პერსონალური ინფორმაციის პოტენციური გაჟონვის კუთხით (მაგალითად, სამედიცინო ჩანაწერების). უსაფრთხოების სისტემებზე თავდასხმების პოტენციური ზარალი შეიძლება იყოს გამოუსწორებელი, არა მხოლოდ ფინანსური ან პირადი რეპუტაციის თვალსაზრისით, როგორც ეს ამჟამად ხდება, არამედ სიცოცხლისთვისაც (მაგალითად, ავტონომიური მართვის პროცესში თავდასხმების შედეგად წარმოქმნილი ფატალური ავარია). გარდა ამისა, ხელოვნური ინტელექტის მიღწევები შეიძლება ბოროტად გამოიყენონ მასობრივი ონლაინთვალთვალისთვის. ამის საპირისპიროდ, ახალი ტექნოლოგიები გვპირდება 6G უსაფრთხოების მნიშვნელოვან გაუმჯობესებას. ბევრ მკვლევარს მიაჩნია, რომ უსაფრთხოების ახალი ტექნოლოგიები იქნება 6G-ის წარმატების მთავარი დებულებები, თუმცა, აღნიშნული მიმართულებით კვლევა ჯერ კიდევ ადრეულ ეტაპზეა.

წინამდებარე წიგნში მიმოხილულია უსაფრთხოების ახალი ტექნოლოგიები 6G ქსელებისთვის, რომელიც მომზადებულია უახლეს პუბლიკაციებსა და სამეცნიერო მიღწევებზე დაყრდნობით. განხილულია 6G ქსელების უსაფრთხოებასთან დაკავშირებული ტექნოლოგიური ტენდენციები, საფრთხეები, გადაწყვეტილებები და ფიზიკური ფენის უსაფრთხოების როლი კონტექსტით გაცნობიერებული უსაფრთხოებისთვის 6G ქსელებში. შესწავლილია მოძრავი სამიზნეების დაცვა, როგორც პროაქტიული თავდაცვის ელემენტი B5G სისტემებისთვის და ენერგოეფექტიანობის თვალსაზრისით ადაპტიური და დინამიკური უსაფრთხოება ხელოვნური ინტელექტის შემცველ 6G ქსელებში. შესწავლილია უსაფრთხოების ფუნქციის ვირტუალიზაცია საგნების ინტერნეტის აპლიკაციებისთვის 6G ქსელებში, ხოლო საგნების ინდუსტრიული ინტერნეტის კუთხით წარმოდგენილია ღრმა სწავლებაზე დაფუძნებული საფრთხის გამოვლენა, რაც ხელს შეუწყობს კრიტიკული ინფრასტრუქტურის დაცვას, და ბლოკჩეინზე დაფუძნებული, სანდო იდენტიფიკატორით ერთობლივი მმართველობის არქიტექტურა. ასევე განხილულია უსაფრთხო ვირტუალური მობილური პატარა ფიჭები და ზონდირების, კომუნიკაციის და უსაფრთხოების ინტეგრირება, როგორც შესაბამისი ნაბიჯები მრავალფუნქციური 6G ქსელებისკენ.

ვფიქრობთ, მასალა სასარგებლო იქნება და დახმარებას გაუწევს საინფორმაციო ტექნოლოგიებისა და კომუნიკაციების დარგში მომუშავე სპეციალისტებს, აკადემიურ პერსონალს, ბაკალავრიატის მაღალი კურსის სტუდენტებს, მაგისტრანტებს, დოქტორანტებს და მათ საერთაშორისო სამეცნიერო ორბიტასთან უდავოდ დაახლოებს.

რამაზ ხუროძე, სერგო შავგულიძე, მამუკა ჩხაიძე

თბილისი, ოქტომბერი, 2022 წელი

ლიტერატურა

პირველ თავში გამოყენებული ლიტერატურა

K. Basu *et al.*, "NIST Post-Quantum Cryptography-A Hardware Evaluation Study," *IACR Cryptol. ePrint Arch.*, vol. 2019, 2019, p. 47.

B. Biggio *et al.*, "Evasion Attacks Against Machine Learning at Test Time," *Proc. Joint Euro. Conf. Machine Learning and Knowledge Discovery in Databases*, Springer, 2013, pp. 387–402.

D. A. Fernandes *et al.*, "Security Issues in Cloud Environments: A Survey," *Int'l. J. Info. Security*, vol. 13, no. 2, 2014, pp. 113–70.

I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and Harnessing Adversarial Examples," *arXiv preprint* arXiv:1412.6572, 2015.

D. Je, J. Jung, and S. Choi, "Toward 6G Security: Technology Trends, Threats, and Solutions", *IEEE Commun. Stand. Mag.*", vol. 5, no. 3, 2021, pp. 64–71.

M. Juuti *et al.*, "Prada: Protecting Against Dnn Model Stealing Attacks," *Proc. IEEE Euro. Symp. Security and Privacy*, 2019, pp. 512–27.

S. Luo *et al.*, "Virtualization Security for Cloud Computing Service," *Proc. Int'l. Conf. Cloud and Service Computing*, 2011, pp. 174–79.

M. Min *et al.*, "Learning-Based Privacy-Aware Offloading for Healthcare IoT With Energy Harvesting," *IEEE Internet of Things J.*, vol. 6, no. 3, 2018, pp. 4307–16.

W. Saad, M. Bennis, and M. Chen, "A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems," *IEEE Network*, vol. 34, no. 3, 2019, pp. 134–42.

R. Shafin *et al.*, "Self-Tuning Sectorization: Deep Reinforcement Learning Meets Broadcast Beam Optimization," *IEEE Trans. Wireless Commun.*, vol. 19, no. 6, 2020, pp. 4038–53.

H. D. Trinh *et al.*, "Mobile Traffic Classification Through Physical Control Channel Fingerprinting: A Deep Learning Approach," *IEEE Transactions on Network and Service Management*, vol. 18, Issue: 2, 2021, pp. 1946–1961.

X. You *et al.*, "Towards 6G *Wireless Communication Networks: Vision, Enabling Technologies, and New Paradigm Shifts," Science* China Info. Sciences, vol. 64, no. 1, 2021, pp. 1–74.

"Samsung 6G White Paper: The Next Hyper-Connected Experience for All," 2020; https://research.samsung.com/next-generation-communications.

მეორე თავში გამოყენებული ლიტერატურა

Y. Arjoune and S. Faruque: "Smart Jamming Attacks in 5G New Radio: A Review," *Proc. 10th Annual Computing and Commun. Wksp. and Conf.*, 2020.

E. Bjorson *et al.*, "MIMO: Ten Myths and One Critical Question," *IEEE Commun. Mag.*, vol. 54, no. 2 2016, pp. 114-23.

A. Bourdoux *et al.*, "6G White Paper on Localization and Sensing," *6G Research Visions*, no. 12, Univ. Oulu, 2020.

X. Chen and L. Lei, "Energy-Efficient Optimization for Physical Layer Security in Multi-Antenna Downlink Networks with QoS Guarantee," *IEEE Commun. Letters*, vol. 17, no. 4, 2013, pp. 637–40.

A. Chorti *et al.*, *Physical Layer Security: A Paradigm Shift in Data Confidentiality, Physical and Data-Link Security Techniques for Future Communication Systems*, Springer, 2016.

A. Chorti *et al.*, "Context-Aware Security for 6G Wireless: The Role of Physical Layer Security," *IEEE Commun. Stand. Mag.*", vol. 6, no. 1, 2021, pp. 102–08.

Z. Md. Fadlullah *et al.*, "GT-QoSec: A Game-Theoretic Joint Optimization of QoS and Security for Differentiated Services in Next Generation Heterogeneous Networks," *IEEE Trans. Wireless Commun.*, vol. 16, no 2, 2017, pp. 1037-50.

M. Mitev *et al.*, "Authenticated Secret Key Generation in Delay-Constrained Wireless Systems," *EURASIP J. Wireless Commun. and Networks*, vol. 122, June 2020, pp. 1-29.

G. A. Nunez Segura *et al.*, "Denial of Service Attacks Detection in Software-Defined Wireless Sensor Networks," *Proc. IEEE ICC Wksp. SDN Security*, 7–11 June 2020, Dublin, Ireland.

H. V. Poor and R. F. Schaefer, "Wireless Physical Layer Security," *Proc. Nat'l. Acad. Sciences of the U.S.A.*, vol. 114, no.1, Jan. 3, 2017, pp. 19–26.

W. Yang, R. F. Schaefer, and H. V. Poor, "Wiretap Channels: Nonasymptotic Fundamental Limits," *IEEE Trans. Info. Theory*, vol. 65, no. 7, 2019, pp. 4069–93.

J. Yao and J. Xu, "Secrecy Yransmission in Large-Scale UAV-Enabled Wireless Networks," *IEEE Trans. Commun.*, vol. 67, no. 11, 2019, pp. 7656–71.

M. Ylianttila *et al.*, "6G White Paper: Research Challenges for Trust, Security and Privacy," *6G Research Visions*, Univ. Oulu, June 2020.

M. Zoli *et al.*, "Physical-Layer-Security Box: A Concept for Time-Frequency Channel-Reciprocity Key Generation," *EURASIP J. Wireless Commun. and Net.*, vol. 122, 2020, pp. 1-24.

3GPP TR33.809, "Study on 5G Security Enhancements Against False Base Stations (Rel 16)," Sept. 2018.

3GPP TR33.825, "Study on the Security of 5G URLLC (Release 16)," Oct. 2019.

მესამე თავში გამოყენებული ლიტერატურა

I. F. Akyildiz, A. Kak, and S. Nie, "6G and Beyond: The Future of Wireless Communications Systems," *IEEE Access*, vol. 8, 2020, pp. 133 995–134 030.

A. Aydeger, N. Saputro, and K. Akkaya, "A Moving Target Defense and Network Forensics Framework for ISP Networks Using SDN and NFV," *Future Generation Computer Systems*, vol. 94, 2019, pp. 496–509.

D. P. Bertsekas, Reinforcement Learning and Optimal Control, Athena Scientific, 2019.

H. Cam, "Cyber Resilience Using Autonomous Agents and Reinforcement Learning," *Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications II*, T. Pham, L. Solomon, and K. Rainey, Eds., vol. 11413, SPIE, 2020, pp. 219–34.

X. Chai *et al.*, "DQMOTAG: Deep Reinforcement Learning-Based Moving Target Defense Against DDoS Attacks," *Proc. 2020 IEEE Fifth Int'l. Conf. Data Science in Cyberspace*, 2020, pp. 375–79.

H. Cho *et al.*, "Toward Proactive, Adaptive Defense: A Survey on Moving Target Defense," *IEEE Commun. Surveys & Tutorials*, vol. 22, no. 1, 2020, pp. 709–45.

A. Chowdhary *et al.*, "MTD Analysis and Evaluation Framework in Software Defined Network (Mason)," *Proc. 2018 ACM Int'l. Wksp. Security in Software Defined Networks and Network Function Virtualization, ser. SDN-NFV Sec'18*, 2018, p. 43–48.

T. Eghtesad, Y. Vorobeychik, and A. Laszka, “Adversarial Deep Reinforcement Learning Based Adaptive Moving Target Defense,“ *Decision and Game Theory for Security*, Q. Zhu et al., Eds., Springer, 2020, pp. 58–79.

Q. Jia, K. Sun, and A. Stavrou, “MOTAG: Moving Target Defense Against Internet Denial of Service Attacks,“ *Proc. 2013 22nd Int’l. Conf. Computer Commun. Networks*, 2013, pp. 1–9.

A. Marzano *et a*l., “The Evolution of Bashlite and Mirai IoT Botnets,“ Proc. 2018 IEEE Symp. Computers and Commun., 2018, pp. 813–18.

J. Ortiz *et al.*, “INSPIRE-5Gplus: Intelligent Security and Pervasive Trust for 5G and Beyond Networks,“ *Proc. 15th ACM Int’l. Conf. Availability, Reliability and Security*, *ser. ARES ’20*, 2020.

W. Soussi, *et al.*, “Moving Target Defense as a Proactive Defense Element for Beyond 5G“, *IEEE Commun. Standards Mag.*“, vol. 5, no. 3, 2021, pp. 72–79.

S. Sengupta *et al.*, “General Sum Markov Games for Strategic Detection of Advanced Persistent Threats Using Moving Target Defense in Cloud Networks,“ *Decision and Game Theory for Security*, T. Alpcan et al., Eds., Springer, 2019, pp. 492–513.

მეოთხე თავში გამოყენებული ლიტერატურა

I. Ahmad *et al.*, “Overview of 5G Security Challenges and Solutions,“ *IEEE Commun. Standards Mag.*, vol. 2, no. 1, 2018, pp. 36–44.

Q. Bi, “Ten Trends in the Cellular Industry and an Outlook on 6G,“ *IEEE Commun. Mag.*, vol. 57, no. 12, 2019, pp. 31–36.

M. Giordani *et al.*, “Toward 6G Networks: Use Cases and Technologies,“ *IEEE Commun. Mag.*, vol. 58, no. 3, 2020, pp. 55–61.

N. Kato *et al.*, “Ten Challenges in Advancing Machine Learning Technologies Toward 6G,“ *IEEE Wireless Commun.*, vol. 27, no. 3, 2020, pp. 96–104.

K. Letaief *et al.*, “The Roadmap to 6G: AI Empowered Wireless Networks,“ *IEEE Commun. Mag.*, vol. 57, no. 8, 2019, pp. 84–90.

M. Mollah *et al.*, “Blockchain for the Internet of Vehicles Towards Intelligent Transportation Systems: A Survey,“ *IEEE Internet of Things J.*, vol. 8, no. 6, 2020, pp. 4157–85.

Z. N. Mowla *et al.*, “AFRL: Adaptive Federated Reinforcement Learning for Intelligent Jamming Defense in FANET,“ *J. Commun. Networks*, vol. 22, no. 3, 2020, pp. 244–58.

S. Shen *et al.*, “Security in Edge-Assisted Internet of Things: Challenges and Solutions,“ *Science China Info. Sciences*, vol. 63, no. 12, 2020, pp. 1–14.

S. Shen *et al.*, “Toward Fast and Accurate SOH Prediction for Lithium-Ion Batteries,“ *IEEE Trans. Energy Conversion*, vol. 36, no. 3, 2021, pp. 2036–46.

S. Shen, C. Yu, K. Zhang, J. Ni, and S. Ci, “Adaptive and Dynamic Security in AI-Empowered 6G: From an Energy Efficiency Perspective,“ *IEEE Commun. Standards Mag.*“, vol. 5, no. 3, 2021, pp. 80–88.

F. Tariq *et al.*, “A Speculative Study on 6G,“ *IEEE Wireless Commun.*, vol. 27, no. 4, Aug. 2020, pp. 118–25

M. Tariq *et al.*, “Vulnerability Assessment of 6G-Enabled Smart Grid Cyber-Physical Systems,“ *IEEE Internet of Things J.*, vol. 8, no. 7, 2020, pp. 5468–75.

J. Zhang *et al.*, “PoisonGAN: Generative Poisoning Attacks Against Federated Learning in Edge Computing Systems,“ *IEEE Internet of Things J.*, vol. 8, no. 5, 2020, pp. 3310–22.

K. Zhang *et al.*, “Security and Privacy for Mobile Healthcare Networks: From a Quality of Protection Perspective,“ *IEEE Wireless Commun.*, vol. 22, no. 4, 2015, pp. 104–12.
Z. Zhang *et al.*, “6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies,“ *IEEE Vehic. Technology Mag.*, vol. 14, no. 3, 2019, pp. 28–41.

მეხუთე თავში გამოყენებული ლიტერატურა

M. N. Aman *et al.*, “Hatt: Hybrid Remote Attestation for the Internet of Things With High Availability,“ *IEEE Internet of Things J.*, vol. 7, no. 8, 2020, pp. 7220–33.
M. N. Aman, M. H. Basheer, and B. Sikdar, “Two-Factor Authentication for Iot With Location Information,“ *IEEE Internet of Things J.*, vol. 6, no. 2, 2019, pp. 3335–51.
M. N. Aman and B. Sikdar, “Att-Auth: A Hybrid Protocol for Industrial Iot Attestation With Authentication,“ *IEEE Internet of Things J.*, vol. 5, no. 6, 2018, pp. 5119–31.
M. N. Aman, U. Javaid, and B. Sikdar, “Security Function Virtualization for IoT Applications in 6G Networks,“ *IEEE Commun. Stand. Mag.*“, vol. 5, no. 3, 2021, pp. 90–95.
C. L. Barrett *et al.*, “Episimdemics: An Efficient Algorithm for Simulating the Spread of Infectious Disease Over Large Realistic Social Networks,“ *Proc. 2008 ACM/IEEE Conf. Supercomputing*, 2008, pp. 1–12.
N. Chen and M. Okada, “Towards 6G Internet of Things and the Convergence With RoF System,“ *IEEE Internet of Things J.*, vol. 8, no. 1, 2021, pp. 8719–33.
S. Cheng *et al.*, “Traffic-Aware Patching for Cyber Security in Mobile IoT,“ *IEEE Commun. Mag.*, vol. 55, no. 7, 2017, pp. 29–35.
N. Guizani *et al.*, “Effects of Social Network Structure on Epidemic Disease Spread Dynamics with Application to Ad Hoc Networks,“ *IEEE Network*, vol. 33, no. 3, 2019, pp. 139–45.
N. Guizani and A. Ghafoor, “A Network Function Virtualization System for Detecting Malware in Large IoT Based Networks,“ *IEEE JSAC*, vol. 38, no. 6, 2020, pp. 1218–28.
U. Javaid *et al.*, “A Scalable Protocol for Driving Trust Management in Internet of Vehicles With Blockchain,“ *IEEE Internet of Things J.*, vol. 7, no. 12, 2020, pp. 11815–29.
M. B. Mollah *et al.*, “Blockchain for the Internet of Vehicles Towards Intelligent Transportation Systems: A Survey,“ *IEEE Internet of Things J.*, vol. 8, no. 6, 2021, pp. 4157–85.
S. Peng, S. Yu, and A. Yang, “Smartphone Malware and Its Propagation Modeling: A Survey,“ *IEEE Commun. Surveys & Tutorials*, vol. 16, no. 2, 2014, pp. 925–41.
E. Ronen and A. Shamir, “Extended Functionality Attacks on IoT Devices: The Case of Smart Lights,“ *Proc. 2016 IEEE Euro. Symp. Security and Privacy*, 2016, pp. 3–12.
N. Ul Hassan, C. Yuen, and D. Niyato, “Blockchain Technologies for Smart Energy Systems: Fundamentals, Challenges, and Solutions,“ *IEEE Industrial Electronics Mag.*, vol. 13, no. 4, 2019, pp. 106–18.
M. Vojnovic and A. J. Ganesh, “On the Race of Worms, Alerts, and Patches,“ I*EEE/ACM Trans. Networking*, vol. 16, no. 5, 2008, pp. 1066–79.

მეექვსე თავში გამოყენებული ლიტერატურა

A. Al-Dulaimi *et al.*, “Adaptive Management of Cognitive Radio Networks Employing Femtocells,“ *IEEE Systems J.*, vol. 11, no. 4, 2017, pp. 2687–98.

A. Alshamrani *et al.*, “A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities,“ *IEEE Commun. Surveys & Tutorials*, vol. 21, no. 2, 2019, pp. 1851–77.

A. Canovas *et al.*, “Multimedia Data Flow Traffic Classification Using Intelligent Models Based on Traffic Patterns,“ *IEEE Network*, vol. 32, no. 6, 2018, pp. 100–07.

J. He *et al.*, “HSI-Bert: Hyperspectral Image Classification Using the Bidirectional Encoder Representation from Transformers,“ *IEEE Trans. Geoscience and Remote Sensing*, vol. 58, no. 1, 2020, pp. 165–78.

Y. P. Hu *et al.*, “Dynamic Defense Strategy Against Advanced Persistent Threat With Insiders,“ *Proc. 2015 IEEE INFOCOM*, 2015, pp. 747–56.

G. K. W. Huang and J. C. Lee, “Hyperpartisan News and Articles Detection Using Bert and Elmo,“ *Proc. 2019 Int’l. Conf. Computer and Drone Applications*, 2019, pp. 29–32.

S. Ji *et al.*, “Parallelizing word2vec in Shared and Distributed Memory,“ *IEEE Trans. Parallel and Distributed Systems*, vol. 30, no. 9, 2019, pp. 2090–2100.

A. Lemay *et al.*, “Survey of Publicly Available Reports on Advanced Persistent Threat Actors,“ *Computers & Security*, vol. 72, 2018, pp. 26–59.

Y. Li *et al.*, “An Intelligence-Driven Security-Aware Defense Mechanism for Advanced Persistent Threats,“ *IEEE Trans. Info. Forensics and Security*, vol. 14, no. 3, 2019, pp. 646–61.

Y. Li *et al.*, “Work Modes Recognition and Boundary Identification of MFR Pulse Sequences With a Hierarchical seq2seq LSTM,“ *IET Radar, Sonar Navigation*, vol. 14, no. 9, 2020, pp. 1343–53.

L. Xiao *et al.*, “Attacker-Centric View of a Detection Game Against Advanced Persistent Threats,“ *IEEE Trans. Mobile Computing*, vol. 17, no. 11, 2018, pp. 2512–23.

K. Yu *et al.*, “Blockchain-Enhanced Data Sharing With Traceable and Direct Revocation in IIoT,“ *IEEE Trans. Industrial Informatics*, vol. 17, no. 11, 2021, pp. 7669-78.

K. Yu *et al.*, “Deep Learning-Based Traffic Safety Solution for a Mixture of Autonomous and Manual Vehicles in a 5G-Enabled Intelligent Transportation System,“ *IEEE Trans. Intelligent Transportation Systems*, vol. 22, no. 7, 2021, 4337– 47.

K. Yu *et al.*, “Securing Critical Infrastructures: Deep-Learning-Based Threat Detection in IIoT,“ *IEEE Commun. Mag.*, vol. 59, no. 10, 2021, pp. 76–82.

J. Zhang *et al.*, “3d Reconstruction for Motion Blurred Images Using Deep Learning-Based Intelligent Systems,“ *Computers, Materials & Continua*, vol. 66, no. 2, 2021, pp. 2087–2106.

C. Zhu *et al.*, “Trust-Based Communication for the Industrial Internet of Things,“ *IEEE Commun. Mag.*, vol. 56, no. 2, 2018, pp. 16–22.

მეშვიდე თავში გამოყენებული ლიტერატურა

M. Al-Bahri *et al.*, “Smart System Based on DOA and IoT for Products Monitoring Anti-Counterfeiting,“ *ICBDSC*, 2019.

R. Huo *et al.*, “A Blockchain-Enabled Trusted Identifier Co-Governance Architecture for the Industrial Internet of Things,“ *IEEE Commun. Mag.*, vol. 60, no. 6, 2022, pp. 66–72.

H. Kalodner *et al.*, “An Empirical Study of Namecoin and Lessons for Decentralized Namespace Design,“ *WEIS*, vol. 1, no. 1, 2015, pp. 1–23.

D. Lang *et al.*, “Pursuing the Vision of Industrie 4.0: Secure Plug-and-Produce by Means of the Asset Administration Shell and Blockchain Technology,“ *IEEE INDIN*, 2018, pp. 1092–97.

D. Liu *et al.*, “Anonymous Reputation System for IIoT-Enabled Retail Marketing ATOP POS Blockchain,“ *IEEE Trans. Ind. Informatics*, vol. 15, no. 6, 2019, pp. 3527–37.

J. Liu *et al.*, “A Data Storage Method Based on Blockchain for Decentralization DNS,“ *IEEE DSC*, July. 2018, pp. 189–96.

Y. Ren *et al.*, “Potential Identity Resolution Systems for the Industrial Internet of Things: A Survey,“ *IEEE Commun. Surveys & Tutorials*, vol. 23, no. 1, 2021, pp. 391-430.

S. Suhail *et al.*, “On the Role of Hash-Based Signatures in Quantum- Safe Internet of Things: Current Solutions and Future Directions,“ *IEEE IoT J.*, vol. 8, no. 1, 2021, pp. 1–17.

S. Wang *et al.*, “Eidm: a Ethereum-Based Cloud User Identity Management Protocol,“ *IEEE Access*, vol. 7, 2021, pp. 115,281–91.

X. Wang *et al.*, “ConsortiumDNS: A Distributed Domain Name Service Based on Consortium Chain,“ *IEEE DSS*, 2017, pp. 617–20.

Y. Wu *et al.*, “Convergence of Blockchain and Edge Computing for Secure and Scalable IIoT Critical Infrastructures in Industry 4.0,“ *IEEE IoT Mag.*, vol. 8, 2019, pp. 2300–17.

H. Xu *et al.*, “A Survey on Industrial Internet of Things: A Cyber-Physical Systems Perspective,“ *IEEE Access*, vol. 6, 2018, pp. 78238–59.

S. Zeng *et al.*, “Survey of Blockchain: Principle, Progress and Application,“ *J. Commun.*, vol. 41, no. 1, 2020, pp. 134–51.

P. Zhang, Y. Wu, and H. Zhu, “Open Ecosystem for Future Industrial Internet of Things (IIoT): Architecture and Application,“ *Csee J Power Energy*, vol. 6, no. 1, 2020, pp. 1–11.

მერვე თავში გამოყენებული ლიტერატურა

W. Chen *et al.*, “Doherty PA for Massive MIMO,“ *IEEE Microwave Mag.*, vol. 21, no. 5, 2020, pp. 78-93.

M. De Ree *et al.,* “Key Management for Beyond 5G Mobile Small Cells: A Survey,“ *IEEE Access,* vol. 7, pp. 59200–36.

M. De Ree *et al.*, “Distributed Trusted Authority-Based Key Management for Beyond 5G Network Coding-Enabled Mobile Small Cells,“ *2019 IEEE 2nd 5GWF*, Dresden, Germany, 2019, pp. 80–85.

S. Irum *et al.*, “Network-Coded Cooperative Communication in Virtualized Mobile Small Cells,“ *2019 IEEE 2nd 5GWF*, Dresden, Germany, 2019, pp. 264–68.

Y. M. Kwon *et al.*, “Performance Evaluation of Moving Small-Cell Network with Proactive Cache,“ *Mobile Information Systems*, vol. 2016, 2016, pp. 1-11.

F. Marzouk, J. P. Barraca, and A. Radwan, “On Energy Efficient Resource Allocation in Shared RANs: Survey and Qualitative Analysis,“ *IEEE Commun. Surveys & Tutorials*, vol. 22, no. 3, 2020, pp. 1515–38.

H. Ning *et al.*, “A Survey and Tutorial on ‘Connection Exploding Meets Efficient Communication’ in the Internet of Things,“ *IEEE Internet of Things J.*, vol. 7, no. 11, 2020, pp. 10733–44.

F. Rebecchi *et al.*, “Data Offloading Techniques in Cellular Networks: A Survey,“ *IEEE Commun. Surveys & Tutorials*, vol. 17, no. 2, 2015, pp. 580–603.

J. Rodriguez *et al.*, “Secure Virtual Mobile Small Cells: A Stepping Stone toward 6G,“ *IEEE Commun. Stand. Mag.*“, vol. 5, no. 6, 2021, pp. 28–36.

M. Sajedin *et al.*, “A Survey on RF and Microwave Doherty Power Amplifier for Mobile Handset Applications,“ *Electronics*, 2019, vol. 8, no. 6, pp. 1–31.

SECRET project (H2020 MCSA-ETN), project no. 722424; http://h2020-secret.eu/.

M. Tayyab *et al.*, "Uplink Reference Signals for Energy-Efficient Handover," *IEEE Access*, vol. 8, 2020, pp. 163060–76.

3GPP TR 36.836 V12.0.0, "Study on Mobile Relay (Release 12)," June 2014.

3GPP TS 22.278 V17.1.0, "Service Requirements for the Evolved Packet System (EPS) (Release 17)," Dec. 2019.

3GPP TS 38.300 V15.0.0. "NR; NR and NG-RAN Overall Description; Stage 2 (Release 15)," Dec. 2017.

მეცხრე თავში გამოყენებული ლიტერატურა

M. Bloch *et al.*, "An Overview of Information-Theoretic Security and Privacy: Metrics, Limits and Applications," *IEEE J. Sel. Topics Info. Theory*, vol. 2, no. 1, 2021, pp. 5–22.

Y. Cui *et al.*, "Integrating Radio Sensing and Communications for Ubiquitous IoT: Applications, Trends and Challenges," *IEEE Network*, vol. 35, no. 5, 2021, pp. 158–67.

A. Hassanien *et al.*, "Dual-Function Radar Communications: Information Embedding Using Sidelobe Control and Waveform Diversity," *IEEE Trans. Signal Process.*, vol. 64, no. 8, 2016, pp. 2168–81.

T. Huang *et al.*, "MAJoRCom: A Dual-Function Radar Communication System Using Index Modulation," *IEEE Trans. Signal Process.*, vol. 68, no. 5, 2020, pp. 3423–38.

M. Kobayashi, G. Caire, and G. Kramer, "Joint State Sensing and Communication: Optimal Tradeoff for a Memory-Less Case," *Proc. IEEE ISIT '18*, Vail, CO, pp. 111–15.

P. Kumari, N. Myers, and R. W. Heath, "Adaptive and Fast Combined Waveform Beamforming Design for mmWave Automotive Joint Communication-Radar," *IEEE J. Sel. Topics Sig. Process.*, vol. 15, no. 4, 2021, pp. 996–1012.

P. Kumari *et al.*, "IEEE 802.11ad-Based Radar: An Approach to Joint Vehicular Communication-Radar System," *IEEE Trans. Vehic. Tech.*, vol. 67, no. 4, 2018, pp. 3012–27.

B. Li, A. P. Petropulu, W. Trappe, "Optimum Co-Design for Spectrum Sharing between Matrix Completion Based MIMO Radars and a MIMO Communication System," *IEEE Trans. Sig. Process.*, vol. 64, no. 7, 2016, pp. 4562–75.

F. Liu *et al.*, "Toward Dual-Functional Radar-Communication Systems: Optimal Waveform Design," *IEEE Trans. Signal Process.*, vol. 66, no. 16, 2018, pp. 4264–79.

N. S. Mannem *et al.*, "A mm-Wave Transmitter MIMO with Constellation Decomposition Array for Key-Less Physical Secured High-Throughput Links," *Proc. IEEE RFIC '21*, Denver, CO, pp. 199–202.

N. Su, F. Liu, and C. Masouros, "Secure Radar-Communication Systems With Malicious Targets: Integrating Radar, Communications and Jamming Functionalities," *IEEE Trans. Wireless Commun.*, vol. 20, no. 1, 2021, pp. 83–95.

M. Tahmasbi, M. Bloch, and A. Yener, "Learning an Adversary's Actions for Secret Communication," *IEEE Trans. Info. Theory*, vol. 66, no. 3, 2020, pp. 1607–24.

Z. Wei *et al.*, "Multi-Cell Interference Exploitation: Enhancing the Power Efficiency in Cell Coordination" *IEEE Trans. Wireless Commun.*, vol. 19, no. 1, 2020, pp. 547–62.

Z. Wei *et al.*, "Toward Multi-Functional 6G Wireless Networks: Integrating Sensing, Communication, and Security," *IEEE Commun. Mag.*, vol. 60, no. 4, 2022, pp. 65–71.

W. Zhang *et al.*, "Joint Transmission and State Estimation: A Constrained Channel Coding Approach," *IEEE Trans. Info. Theory*, vol. 57, no. 10, 2011, pp. 7084–95.

აბრევიატურები და აკრონიმები

3GPP – Third Generation Partnership Project – მე-3 თაობის პარტნიორობის პროექტი

4C – Computation, Communication, Caching, Control – გამოთვლები, კომუნიკაცია, ქეშირება და კონტროლი

6LoWPAN – IPv6 over Low-Power Wireless Personal Area Networks – IPv6 დაბალი სიმძლავრის უსადენო პერსონალურ ქსელებზე

AAS – Asset Administration Shell – აქტივების ადმინისტრირების გარსი

AES – Advanced Encryption Algorithm – დაშიფვრის მოწინავე ალგორითმი

AI – Artificial Intelligence – ხელოვნური ინტელექტი

AIoT – Artificial Intelligence of Things – საგნების ხელოვნური ინტელექტი

AKA – Authentication and Key Agreement – ავთენტიფიკაცია და გასაღებების შესახებ შეთანხმება

AML – Adversarial Machine Learning – შეჯიბრებითი მანქანური სწავლება

AoA – Angle of Arrival – (ტალღის) მოსვლის კუთხე

AP – Access Point – წვდომის წერტილი

API – Application Programming Interface – აპლიკაციის პროგრამირების ინტერფეისი

APT – Advanced Persistent Threat – მოწინავე მუდმივი საფრთხე

ARQ – Automatic Repeat Request – ავტომატური განმეორებითი მოთხოვნა

B5G – Beyond 5G – 5G-ის შემდგომი

BBU – Baseband Units – საბაზისო სიგნალების ბლოკები

BERT – Bidirectional Encoder Representations from Transformers – ორმხრივი კოდერის წარმოდგენები ტრანსფორმერებისგან

BLE – Bluetooth Low Energy – დაბალი ენერგიის Bluetooth

BS – Base Station – საბაზო სადგური

CAPEX – Capital Expenditure – კაპიტალური დანახარჯები

CAPIF – Common Application Programming Interface Framework – აპლიკაციის პროგრამირების საერთო ინტერფეისის სტრუქტურა

CCTV – Closed Circuit Television – დახურული ტელევიზია

CDA – Constellation Decomposition Array – კონსტელაციის დაშლის მასივი

CI – Constructive Interference – კონსტრუქციული ინტერფერენცია

CNN – Convolutional Neural Network – კონვოლუციური ნეირონული ქსელი

CO – Cell Offloading – ფიჭის გადმოტვირთვა

CPU – Central Processing Unit – ცენტრალური პროცესორი

CRAN – Cloud RAN – ღრუბლოვანი RAN

CRSS – Communication and Radar Spectrum Sharing – საკომუნიკაციო და სარადარო სპექტრის გაზიარება

CSI – Channel State Information – არხის მდგომარეობის შესახებ ინფორმაცია

D – Dimension – განზომილება

D2D – Device-to-Device – მოწყობილობებს შორის (კომუნიკაცია)

DAC – Digital-to-Analog Converter – ციფრულ-ანალოგური გარდამქმნელი

DB – Data Base – მონაცემთა ბაზა

DDoS – Distributed Denial of Service – სერვისზე განაწილებული უარის თქმა

DeNB – Donor eNB – დონორი eNB

DES – Data Encryption Standard – მონაცემთა შიფრირების სტანდარტი

DL – Deep Learning – ღრმა სწავლება

DM – Directional Modulation – მიმართულებითი მოდულაცია

DN – Destination Node – დანიშნულების კვანძი

DNN – Deep Neural Network – ღრმა ნეირონული ქსელი

DNS – Domain Name System – დომენის სახელების სისტემა

DoS – Denial of Service – სერვისზე უარის თქმა

DPA – Doherty PA – დოჰერტის PA

DRL – Deep Reinforcement Learning – ღრმა განმტკიცებული სწავლება

E2E – End-to-End – ბოლო პუნქტების (დამაკავშირებელი)

EAP-TLS – Extensible Authentication Protocol-Transport Layer Security – გაფართოებადი ავთენტიფიკაციის პროტოკოლ-ტრანსპორტის ფენის უსაფრთხოება

eNB – evolved NodeB – განვითარებული NodeB

ERLLC – Enhanced RLLC – გაუმჯობესებული RLLC

ERN – Enterprise Registration Node – საწარმოთა რეგისტრაციის კვანძი

ETSI – European Telecommunications Standards Institute – ევროპის სატელეკომუნიკაციო სტანდარტების ინსტიტუტი

eURLLC – enhanced URLLC – გაუმჯობესებული URLLC

FBS – False BS – ყალბი BS

FD-TTP – Fully Distributed TTP – სრულად განაწილებული TTP

FeMBB – Further-enhanced Mobile Broadband – კიდევ უფრო გაუმჯობესებული მობილური ფართოზოლოვანი (ქსელი)

FG – Focus Group – ფოკუს ჯგუფი

G – Generation – თაობა

GaAs – Gallium Arsenide – გალიუმის არსენიდი

GCM – Galois Counter Mode – გალუას მრიცხველის რეჟიმი

GHR – Global Handle Registry – ჰენდლის გლობალური რეგისტრი

GPU – Graphics Processing Unit – გრაფიკული დამუშავების ბლოკი

GR – Group Report – ჯგუფის ანგარიში

GS – Group Specification – ჯგუფის სპეციფიკაცია

GSMA – Global System for Mobile Communications Association – მობილური კომუნიკაციების გლობალური სისტემის ასოციაცია

GUTI – Globally Unique Temporary Identifier – გლობალურად უნიკალური დროებითი იდენტიფიკატორი

HARQ – Hybrid ARQ – ჰიბრიდული ARQ

Hatt – Hybrid attestation – ჰიბრიდული ატესტაცია

HLA – High-Level Architecture – მაღალი დონის არქიტექტურა

HMI – Human-Machine Interface – ადამიანი-მანქანის ინტერფეისი

HNV – Holistic Network Virtualization – ქსელის ჰოლისტიკური ვირტუალიზაცია

HO – Handover – ჰენდოვერი

HTTP – Hypertext Transfer Protocol – ჰიპერტექსტის გადაცემის პროტოკოლი

HW – Hardware – აპარატურული უზრუნველყოფა

IAB – Integrated Access and Backhaul – ინტეგრირებული წვდომა და ბექჰოლი

IC – Integrated Circuit – ინტეგრალური სქემა

ICS-CERT – Industrial Control Systems Cyber Emergency Response Team – იდუსტრიული მართვის სისტემების საგანგებო კიბერსიტუაციებზე რეაგირების ჯგუფი

ICT – Information and Communication Technology – საინფორმაციო და საკომუნიკაციო ტექნოლოგიები

ID – Identifier – იდენტიფიკატორი

IDS – Intrusion Detection System – შეჭრის აღმოჩენის სისტემა

IED – Intelligent Electronic Device – ინტელექტუალური ელექტრონული მოწყობილობა

IEEE – Institute of Electrical and Electronics Engineers – ელექტრო და ელექტრონიკის ინჟინრების ინსტიტუტი

IIoT – Industrial IoT – ინდუსტრიული IoT

IMEI – International Mobile Equipment Identity – მობილური მოწყობილობის საერთაშორისო იდენტიფიკაცია

IoE – Internet of Everything – ყველაფრის ინტერნეტი

IoT – Internet of Things – საგნების ინტერნეტი

IP – Internet Protocol – ინტერნეტ-პროტოკოლი

IPS – Intrusion Prevention System – შეჭრის პრევენციის სისტემა

IPSec – Internet Protocol Security – ინტერნეტ-პროტოკოლის უსაფრთხოება

ISAC – Integrated Sensing And Communication – ინტეგრირებული ზონდირება და კომუნიკაცია

ISG – Industrial Specification Group – ინდუსტრიული სპეციფიკაციის ჯგუფი

ISN – Identifier Service Node – საიდენტიფიკაციო სერვისის კვანძი

ITU – International Telecommunication Union – ტელეკომუნიკაციის საერთაშორისო კავშირი

ITU-T – ITU-ის სტანდარტიზაციის სექტორი

KM – Key Management – გასაღების მართვა

KPI – Key Performance Indicator – ძირითადი მახასიათებლების ინდიკატორი

LDPC – Low-Density Parity-Check – დაბალი სიმკვრივის ლუწობის შემმოწმებელი (კოდი)

LHS – Local Handle Service – ჰენდლის ლოკალური სერვისი

LO – Local Oscillator – ადგილობრივი ოსცილატორი

LoS – Line of Sight – პირდაპირი ხედვის ხაზი

LSTM – Long Short-Term Memory – გრძელი მოკლევადიანი მეხსიერება

LTE – Long-Term Evolution – გრძელვადიანი ევოლუცია

LU – Legitimate User – ლეგიტიმური მომხმარებლები

MAC – Medium Access Control – გარემოსთან წვდომის მართვა

MANET – Mobile ad hoc Network – მობილური ad hoc (სპეციალური) ქსელი

MCH – Mobile Cell Head – ფიჭის მობილური თავი (მოწყობილობა)

MCN – Mobile Core Network – ძირითადი მობილური ქსელი

MDP – Markov Decision Process – მარკოვის გადაწყვეტილების პროცესი

MEC – Mobile Edge Computing – მობილური პერიფერიული გამოთვლები

MIMO – Multiple Input Multiple Output – მრავალშესასვლელიანი და მრავალგამოსასვლელიანი (ტექნოლოგია)

MISO – Multiple Input Single Output – მრავალშესასვლიანი და ერთგამოსასვლელიანი (ტექნოლოგია)

MitM – Man-in-the-Middle – კაცი შუაში

ML – Machine Learning – მანქანური სწავლება

MM – Mobility Management – მობილურობის მართვა

MME – Mobility Management Entity – მობილურობის მართვის ერთეული

MMIC – Monolithic Microwave IC – მონოლითური მიკროტალღური IC

mMIMO – massive MIMO – მასიური MIMO

mMTC – Massive Machine-Type Communication – მასობრივი მანქანის ტიპის კომუნიკაცია

MNO – Mobile Network Operator – მობილური ქსელის ოპერატორი

MPA – Multi-Primary Administrators – მრავალი ძირითადი ადმინისტრატორები

MR – Mobile Relay – მობილური სარელეო

MRAT – Multiple RAT – მრავალჯერადი RAT

MRN – Mobile Relay Node – მობილური სარელეო კვანძი

MSC – Mobile Small Cell – მობილური პატარა ფიჭა

MTD – Moving Target Defense – მოძრავი სამიზნეების დაცვა

MTU – Master Terminal Unit – მთავარი ტერმინალური ბლოკი

MVNO – Mobile Virtual Network Operator – მობილური ვირტუალური ქსელის ოპერატორი

NC – Network Coding – ქსელური კოდირება

NCC – Network Coded Cooperation – ქსელის კოდირებული კოოპერაცია

NE – Network Entity – ქსელის ერთეული

NEF – Network Exposure Function – ქსელის ექსპოზიციის ფუნქცია

NF – Network Function – ქსელის ფუნქცია

NFC – Near Field Communication – ახლო ველის კომუნიკაცია

NFV – Network Function Virtualization – ქსელის ფუნქციის ვირტუალიზაცია

NFV MANO – NFV Management and Orchestration – NFV მენეჯმენტი და ორკესტრირება

NFVI – NFV Infrastructure – NFV ინფრასტრუქტურა

NFVO – NFV Orchestrator – NFV ორკესტრატორი

NIST – National Institute of Standards and Technology – სტანდარტებისა და ტექნოლოგიების ეროვნული ინსტიტუტი

NMN – Network Management Node – ქსელის მართვის კვანძი

nRT RIC – near-Real-Time RIC – RIC თითქმის რეალურ დროში

NRT RIC – Non-Real-Time RIC – RIC არარეალურ დროში

NSE-H – Network Security Engine-Hypervisor – ქსელის უსაფრთხოების ძრავის ჰიპერვიზორი

NWDAF – Network Data Analytics Function – ქსელის მონაცემთა ანალიზის ფუნქცია

OFDM – Orthogonal Frequency Division Multiplexing – მულტიპლექსირება ორთოგონალური სიხშირული დაყოფით

ONAP – Open Network Automation Platform – ღია ქსელის ავტომატიზაციის პლატფორმა

OPEX – Operational Expenditure – საოპერაციო დანახარჯები

OptSFC – Optimizer for Security Functions – უსაფრთხოების ფუნქციების ოპტიმიზატორი

ORAN – Open RAN – ღია RAN

OS – Operating System – ოპერაციული სისტემა

OSS/BSS – Operating/Business Support System – ოპერაციული/ბიზნესის მხარდაჭერის სისტემა

OSSM – OSS/BSS Manager – OSS/BSS მენეჯერი

OTA – Over-The-Air – ჰაერით (უსადენო გადაცემა)

PA – Power Amplifier – სიმძლავრის გამაძლიერებელი

PD-TTP – Partially Distributed TTP – ნაწილობრივ განაწილებული TTP

PGW – Packet Data Network Gateway – მონაცემთა პაკეტის ქსელის კარიბჭე

pHEMT – pseudomorphic High-Electron-Mobility-Transistor – მაღალი მობილურობის ფსევდომორფული ტრანზისტორი

PHY – Physical – ფიზიკური (ფენა)

PKI – Public Key Infrastructure – საჯარო გასაღების ინფრასტრუქტურა

PLC – Programmable Logic Controller – პროგრამირებადი ლოგიკური კონტროლერი

PLS – Physical Layer Security – ფიზიკური ფენის უსაფრთხოება

PQC – Post-Quantum Cryptography – პოსტკვანტური კრიპტოგრაფია

ProSe – Proximity Service – სიახლოვის სერვისი

PS – Phase Shifter – ფაზამაბრუნი

PUF – Physical Unclonable Function – ფიზიკური არაკლონირებადი ფუნქცია

QAM – Quadrature Amplitude Modulation – კვადრატული ამპლიტუდური მოდულაცია

QC – Quantum computing – კვანტური გამოთვლები

QoE – Quality of Experience – გამოცდილების ხარისხი

QoS – Quality of Service – სერვისის ხარისხი

QoSec – Quality of Security – უსაფრთხოების ხარისხი

QPSK – Quadrature Phase Shift Keying – კვადრატული ფაზური მოდულაცია

RAN – Radio Access Network – რადიოწვდომის ქსელი

RAT – Radio Access Technology – რადიოწვდომის ტექნოლოგია

RC4 – Rivest Cipher 4 – რივესტ-შიფრატორი 4

RF – Radio Frequency – რადიოსიხშირე

RIC – RAN Intelligent Controller – RAN-ის ინტელექტუალური კონტროლერი

RL – Reinforcement Learning – განმტკიცებული სწავლება

RLLC – Reliable Low Latency Communication – საიმედო დაბალი შეყოვნების კომუნიკაცია

RLNC – Random Linear Network Coding – ქსელის შემთხვევითი წრფივი კოდირება

RlUE – Relay UE – სარელეო UE

RM – Resource Management – რესურსების მართვა

RmUE – Remote UE – დისტანციური UE

RN – Relay Node – სარელეო კვანძი

RNTI – Radio Network Temporary Identifier – რადიოქსელის დროებითი იდენტიფიკატორი

ROC – Receiver Operating Characteristic – მიმღების ოპერაციული მახასიათებელი

RRC – Radio Resource Control – რადიორესურსების მართვა

RRH – Remote Radio Head – დისტანციური რადიოთავი (მოწყობილობა)

RRM – Resource Management – რადიორესურსების მართვა

RS – Reference Signal – საცნობარო სიგნალი

RSA – Rivest-Shamir-Adleman – რივესტ-შამირ-ადლემანის (ალგორითმი)

RTU – Remote Terminal Unit – დისტანციური ტერმინალური ერთეული

SA – Security Agent – უსაფრთხოების აგენტი

SAI – Securing Artificial Intelligence – ხელოვნური ინტელექტის უსაფრთხოების უზრუნველყოფა

SC – Small Sell – პატარა ფიჭა

SCADA – Supervisory Control and Data Acquisition – საზედამხედველო კონტროლი და მონაცემთა მოპოვება

SCNR – Signal-to-Clutter-plus-Noise Ratio – სიგნალის ხელშეშლა-პლუს-ხმაურთან თანაფარდობა

SDN – Software Defined Networking – SW-ით განსაზღვრული ქსელი

SEC – Security – უსაფრთხოება

SECRET-MSC – SEcure Network Coding for Reduced Energy nexT generation Mobile Small Cells – უსაფრთხო ქსელური კოდირება შემცირებული ენერგიით შემდეგი თაობის პატარა ფიჭებისთვის

SEPP – Security Edge Protection Proxy – პერიფერიული უსაფრთხოების დაცვის პროქსი-სერვერი

SFV – Security Function Virtualization – უსაფრთხოების ფუნქციის ვირტუალიზაცია

SGW – Serving Gateway – მომსახურების კარიბჭე

SHA – Secure Hash Algorithms – უსაფრთხო ჰეშირების ალგორითმები

SIM – Subscriber Identity Module Card – აბონენტის იდენტიფიკაციის მოდულის ბარათი

SINR – Signal-to-Interference-plus-Noise Ratio – სიგნალის ინტერფერენცია-პლუს-ხმაურთან თანაფარდობა

SKG – Secret Key Generation – საიდუმლო გასაღების გენერაცია

SLA – Service Level Agreement – სერვისის დონის შეთანხმება

SM – Security Manager – უსაფრთხოების მენეჯერი

SN – Source Node – წყაროს კვანძი

SQL – Structured Query Language – სტრუქტურირებული შეკითხვების ენა

SRV – Server – სერვერი

SSH – Secure Shell – უსაფრთხო გარსი

SSLA – Security Service Level Agreement – უსაფრთხოების სერვისის დონის შეთანხმება

SVM – Support Vector Machine – დამხმარე ვექტორული მანქანა

SW – Software – პროგრამული უზრუნველყოფა

TCO – Total Cost of Ownership – საკუთრების მთლიანი ღირებულება

TCP – Transmission Control Protocol – გადაცემის მართვის პროტოკოლი

TDM – Time Division Multiplexing – მულტიპლექსირება დროითი დაყოფით

TDMA – Time Division Multiple Access – მრავალჯერადი წვდომა დროითი დაყოფით

THD – Trusted Handle Data – ჰენდლის სანდო მონაცემები

TICA – Trusted Identifier Co-governance Architecture – სანდო იდენტიფიკატორით ერთობლივი მმართველობის არქიტექტურა

TL – Trust Level – სანდოობის დონე

TPM – Trusted Platform Module – სანდო პლატფორმის მოდული

TR – Technical Report – ტექნიკური ანგარიში

TTP – Trusted Third Party – სანდო მესამე მხარე

UAV – Unmanned Aerial Vehicle – უპილოტო საფრენი აპარატი

UE – User Equipment – მომხმარებლის მოწყობილობა

UHD – Untrusted Handle Data – ჰენდლის არასანდო მონაცემები

UL – Uplink – აპლინკი

UL RS – UL Reference Signal – UL-ის საცნობარო სიგნალი

umMTC – ultra-massive Machine Type Communication – ულტრა მასობრივი მანქანური ტიპის კომუნიკაცია

URLLC – Ultra-Reliable Low-Latency Communication – ულტრა საიმედო დაბალი შეყოვნების კომუნიკაცია

VIM – Virtual Infrastructure Manager – ინფრასტრუქტურის ვირტუალური მენეჯერი

VLC – Visible Light Communications – ხილული სინათლით კომუნიკაცია

VM – Virtual Machine – ვირტუალური მანქანა

VMI – Virtual Machine Introspection – ვირტუალური მანქანის თვითანალიზი

vMSC – virtualized MSC – ვირტუალიზებული MSC

VNF – Virtual Network Function – ვირტუალური ქსელის ფუნქცია

VNFM – VNF Manager – VNF მენეჯერი

VPN – Virtual Private Network – ვირტუალური კერძო ქსელი

VR – Virtual Reality – ვირტუალური რეალობა

vRAN/vCore – ვირტუალური RAN/ვირტუალური Core

VRM – Virtual Resource Management – ვირტუალური რესურსების მართვა

WAN – Wide Area Network – გლობალური ქსელი

WiFi Direct – პირდაპირი WiFi

WIM – WAN Infrastructure Manager – WAN-ის ინფრასტრუქტურის მენეჯერი

WLAN – Wireless Local-Area Network – უსადენო ადგილობრივი ქსელი

XR – eXtended Reality – გაფართოებული რეალობა

ZSM – Zero touch network and Service Management – ნულოვანი შეხების ქსელის სერვისების მენეჯმენტი

ZT – Zero Trust – ნულოვანი სანდოობა