МРНТИ 81.93.29
УДК 004.056.5

https://doi.org/10.51889/2021-4.1728-7901.03

А.Ж. Иманбаев[1], С. Тынымбаев[2], Р.С. Одарченко[3], Ж.Алиханқызы[4]*

[1] әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қ, Қазақстан
[2]Ғұмарбек Дәукеев атындағы Алматы энергетика және байланыс университеті, Алматы қ, Қазақстан
[3] Ұлттық Авиациялық Университет, Киев қ., Украина
[4] Қазақстан-Британ Техникалық университеті, Алматы қ, Қазақстан
**e-mail: imanbaevazamat@gmail.com*

БЕСІНШІ БУЫН МОБИЛЬДІ ЖЕЛІЛЕРДІҢ ҚАУІПСІЗДІК МӘСЕЛЕЛЕРІН ТАЛДАУ

Аңдатпа

Әзірге 5G мобильді желілерін дамыту қауіпсіздікке айтарлықтай әсер етеді. 3GPP 5G стандарты радиоқабылдау желісі мен желінің өзегі арасындағы физикалық және виртуалды қабаттасулардың әртүрлі түрлеріне мүмкіндік беретін жеткілікті икемді. Радиоқабылдау желісі мен ядро арасындағы функцияларды бөлу бәсекеге қабілеттілік пен өнімділік туралы сұрақтарды тудырады. Бұл мақала алдымен 5G қауіпсіздік талаптарын, соның ішінде бизнес қолданбаларға, желі архитектурасына, радиоинтерфейсіне және пайдаланушы құпиялылығына арналған қауіпсіздік талаптарын қарастырады. Осының негізінде ағымдағы мобильді қауіпсіздік архитектурасының алдында тұрған мәселелер талданады және ішкі қауіпсіздік элементтері желі архитектурасы тұрғысынан қарастырылады. Кейіннен 5G желісі мен радиоинтерфейс технологияларындағы инновациялар әкелген қауіпсіздік ресурстары мен техникалық сипаттамаларын ескере отырып, 5G қауіпсіздігін қосымша қолдауға арналған негізгі технологияларды, оның ішінде физикалық деңгей қауіпсіздігін, шифрлауды және пайдалануды қоса алғанда, ғылыми-зерттеу және әзірлеу үрдістерінің ағымдағы жай-күйі. 5G-дегі блокчейн технологиясы, сонымен қатар 5G желілерін қорғау бойынша кейбір қарсы шаралар мен ұсыныстар ұсынылған.

Түйін сөздер: 5G, заттар интернеті, виртуализация, шеткі есептеулер, 3GPP, блокчейн.

Аннотация

А.Ж. Иманбаев[1], С. Тынымбаев[2], Р.С. Одарченко[3], Ж. Алиханкызы[4]
[1] Казахский национальный университет имени аль-Фараби, г. Алматы, Казахстан
[2] Алматинский университет энергетики и связи имени Гумарбека Даукеева, г. Алматы, Казахстан
[3] Национальный Авиационный Университет, г. Киев, Украина
[4] Казахстанско-Британский Технический Университет, г. Алматы, Казахстан

АНАЛИЗ ПРОБЛЕМ БЕЗОПАСНОСТИ МОБИЛЬНЫХ СЕТЕЙ ПЯТОГО ПОКОЛЕНИЯ

На данный момент развитие мобильных сетей 5G окажут значительное влияние на безопасность. Стандарт 5G 3GPP является независимым в том смысле, что он достаточно гибок, чтобы допускать различные типы физического и виртуального перекрытия между сетью радиодоступа и ядром сети. Разделение функций между сетью радиодоступа и ядром поднимает вопросы о конкурентоспособности и производительности. В этой статье сначала рассматриваются требования безопасности 5G, в том числе требования безопасности для бизнес-приложений, сетевой архитектуры, радиоинтерфейса и конфиденциальности пользователей. На этой основе анализируются проблемы, с которыми сталкивается существующая архитектура безопасности мобильной связи, и изучаются внутренние элементы безопасности с точки зрения сетевой архитектуры. Впоследствии, с учетом ресурсов безопасности и технических характеристик, привнесенных инновациями в технологии сетей и радиоинтерфейсов 5G, представлены текущее состояние исследований и тенденции развития основных технологий дополнительной поддержки безопасности 5G, включая безопасность физического уровня, шифрование и применение технологии блокчейн в 5G, так же предложены некоторые контрмеры и предложения по защите сетей 5G.

Ключевые слова: 5G, Интернет вещей, виртуализация, граничные вычисления, 3GPP, блокчейн.

Abstract

ANALYSIS OF THE SECURITY PROBLEMS OF FIFTH GENERATION MOBILE NETWORKS

Imanbayev A.Zh.[1], Tynymbayev S.[2], Odarchenko R.S. [3], Alikhankyzy Zh.[4]

[1] Al-Farabi Kazakh National University, Almaty, Kazakhstan

[2] University of Energy and Communications named after Gumarbek Daukeev

[3] National Aviation University, Kiev, Ukraine

[4] Kazkh-British Technical University, Almaty, Kazakhstan

For now, the development of 5G mobile networks will have a significant impact on security. The 3GPP 5G standard is independent in the sense that it is flexible enough to allow for different types of physical and virtual overlap between the radio access network and the core of the network. The separation of functions between the radio access network and the core raises questions about competitiveness and performance. This article first looks at the security requirements of 5G, including security requirements for business applications, network architecture, air interface, and user privacy. On this basis, the challenges faced by the current mobile security architecture are analyzed and internal security elements are examined from a network architecture perspective. Subsequently, taking into account the security resources and technical characteristics brought by innovations in 5G network and radio interface technologies, the current state of research and development trends of the main technologies for additional 5G security support, including physical layer security, encryption and the use of blockchain technology in 5G, are presented, as well as some countermeasures and proposals to protect 5G networks.

Keywords: 5G, Internet of Things, virtualization, edge computing, 3GPP, blockchain.

Кіріспе

Ұялы байланыс технологиясының жаңа буыны ретінде, 5G адамдар арасындағы қарым-қатынас үшін ғана емес, сонымен қатар адамдар мен заттар арасындағы қарым-қатынас үшін де, ақылды заттар арасында да шынайы "жан-жақты қамтылған Интернетті" (Internet of Everything) жүзеге асыру үшін қолданылады. 5G ұялы байланысын Қазақстанда жүзеге асыру, миллиардтаған құрылғылардың тоқтаусыз жұмыс жасауын қамтамасыз етеді. Ол желілерге жаңа талаптардың қойылуына әкеледі [1].

5G дәстүрлі желілерге қарағанда жоғары жылдамдық, төмен қуат тұтыну, қысқа кідіріс және кең қосылыстардың сипаттамаларына ие. Сонымен қатар, мобильді интернеттің мүмкіндіктерін едәуір жақсарту негізінде 5G Заттар интернетіне дейін кеңейе түсті, ал оның қызмет көрсету мақсаттары адамдардың адамдармен тілдесуінен, адамдар мен заттардың тілдесуіне және де заттардан заттарға дейін кеңейе түсті. Заттардың байланысы барлық нәрсенің өзара байланысының жаңа дәуірін ашады. 5G желілерін құруда қажет ететін кеңейтілген мобильді кеңжолақты байланыс (eMBB), машина типіндегі жаппай байланыс (mMTC) және өте сенімді кідіріс байланысы секілді (uRLLC) үш негізгі қызметті қамтиды [2].

Алдыңғы 2G, 3G және 4G (LTE) жағдайларындағыдай, 5G желілері мен байланыс қызметтері үшін қауіпсіздік өте маңызды, өйткені мобильді жүйелер, қазіргі уақытта бүкіл әлем бойынша миллиардтаған адамдарға қосылуды қамтамасыз етеді. Сонымен қатар, ұялы байланыс желісі интеллектуалды желілерді, алғашқы жауап қату бөлімшелерін (First Responder Units) және алдыңғы қатарлы әскери өзін-өзі ұйымдастыратын желілерді қоса алғанда, қазіргі заманғы жаңа маңызды инфрақұрылымның іргетасы болып табылады [3]. 5G-дің пайда болуымен жаңа желілер мен қосымшалар, соның ішінде автономды жүргізуге арналған жаңа буын автомобиль желілері, ақылды қалалар мен ақылды қауымдастықтар пайда болды.

Қауіп-қатер ландшафты тез өзгереді және шабуылдар басқа қосылу нүктелерінен туындауы мүмкін. Соңғы уақытқа дейін бұл теориялық қауіп болды. Соңғы онжылдықта серіктестік желілерден немесе радио қол жетімділік желілерінен (RAN) шабуылдар болуы мүмкін болдаммен көптеген ғылыми зерттеулер жарияланғанына қарамастан, бұл қауіптер қазіргі кезде өзекті болып табылады. Сол кезде заттар интернетінің қарқынды өсуі шабуылдаушылар құрылғыларды өз бақылауына алып, оларды қызмет жеткізушісіне қарсы қару ретінде пайдалану қаупіне ұшырайды. WireX және т.б. сияқты бірнеше ботнеттер табылып, жойылды [4]. Әзірге бұл шабуылдар интернеттегі түйіндерге бағытталған, бірақ бұл тек уақыт мәселесі, олар EPC (Evolved Packet Core) компоненттеріне шабуыл жасай бастайды. Бұрын жеке және жеке меншік протоколдардың артында жасырылған бұл компоненттер қазір IP, UDP немесе SCTP-де орналасқан, оларды қарапайым техникалық «қызмет көрсетуден бас тарту» шабуылдарымен өшіруге болады. Шабуыл беті бұрынғыға қарағанда едәуір үлкен және қауіпсіздікке ескірген тәсілдер жұмыс істемейді. Сигналдық дауыл сияқты DDoS шабуылын шабуылдаушы немесе тіпті заңды дереккөз жасай алады. Мысалы, IoT құрылғысында

дұрыс жұмыс істемейтін протокол стегі сигнал дауылының генерациясының кесірінен істен шығуы мүмкін.

5G желілерінің, әсіресе жаңа 5G қызметтерінің, жаңа архитектуралардың және жаңа технологиялардың даму үрдісі пайдаланушылардың қауіпсіздігі мен құпиялылығын қорғау саласында жаңа міндеттер тудырады. Бұл мақалада 5G бизнес қолданбаларының қауіпсіздік талаптары, желі архитектурасы, радио интерфейсі және пайдаланушы құпиялылығы талданады. 5G қауіпсіздік архитектурасының даму тенденциялары 5G қауіпсіздігін дамытудағы жаңа тренд болып табылатын ішкі қорғаныс архитектурасына баса назар аудара отырып жинақталған. Бірнеше қосымша 5G қауіпсіздік технологиялары қаралды, соның ішінде физикалық деңгей қауіпсіздігі, жеңіл шифрлау, желі сегментінің қауіпсіздігі, пайдаланушының құпиялылығын қорғау және 5G-ге қолданылатын блокчейн технологиясы және 5G желілерін қорғау байланысты ұсыныстар жасалды [5].

Жалпы қауіпсіздік талаптары 5G

Жаңа бизнес қосымшаларынан туындаған қауіпсіздік талаптары.

5g үш қолданбалы сценарий үшін әртүрлі қауіпсіздік талаптары бар қорғаныс механизмдерін қамтамасыз етуі керек: eMBB, mMTC және uRLLC [6]. eMBB өткізу қабілеті мен пайдаланушының тәжірибесіне өте жоғары талаптар қоятын қызметтерге назар аударады, ал әр түрлі қызметтер үшін қауіпсіздік талаптары әр түрлі; mmtc терминалдың ресурстары мен энергия шығыны шектеулі болған кезде жоғары тығыздықтағы сценарийлерге назар аударады, ол жеңіл қауіпсіздік алгоритмдерін, қарапайым және тиімді қауіпсіздік хаттамаларын қажет етеді; uRLLC төмен кідіріс және жоғары қауіпсіздік қызметтеріне назар аударады және қосымша байланыс кідіріссіз жоғары деңгейдегі қорғаныс шараларын қажет етеді. Жаңа 5G қызметтері мен жаңа сценарийлердің қосымшаларына қойылатын талаптар шектеулі есептеу ресурстарымен, көлемімен және қуат тұтынуымен байланысты шектеулермен бірге 5G қауіпсіздігін неғұрлым күрделі мәселелерге қояды. 5G ішкі қауіпсіздік тетіктерін үйрену-бұл қауіпсіздікке жаңа көзқарас.

Жаңа желілік архитектурадан туындаған қауіпсіздік талаптары.

Жаңа 5G желілік архитектурасы басқару жазықтығы мен құрылғының деректер жазықтығын бөлетін (SDN, Software Defined Network) және желілік функцияларды виртуализациялау (NFV, желілік функцияларды виртуализациялау) технологияларын ұсынады [3], интеграцияға арналған бірнеше өндірушілердің жалпы АТ-аппараттық платформасы негізделген, бірақ ол сонымен қатар көптеген қауіпсіздік мәселелерін тудырады: біріншіден, пайдаланушыларды баптау және ресурстарды визуализациялауға арналған қосымшалар бұлтты платформаның қауіпсіздігі мен сенімділігіне қауып тудырады; екіншіден, есептеулерді, қоймаларды және желілік ресурстарды бірігіп пайдалану виртуалды машиналардың қауіпсіздігі, виртуализация бағдарламалық жасақтамасының қауіпсіздігі және деректердің қауіпсіздігі сияқты міселерлі тудырады; сондай-ақ, орналастыру орталықтандырылған және жалпы мақсаттағы жабдықтар вирустардың орталықтандырылған өрісте тез таралуына әкеледі, ал аппараттық осалдықтарды зиянкестер анықтап, қолдана алады. Осылайша, априорлық білімге негізделген дәстүрлі қорғаныс моделі ендігі 5G дамуына бейімделе алмайды. 5G желісінің ішкі қауіпсіздік атрибуттарын зерттеу үшін 5G желілік архитектурасының шарттарын зерттеу қажет. 5G ішкі қауіпсіздігінің негізгі технологияларын және сенімсіз желілік компоненттерді түсіну жоғары сенімді және ақауларға төзімді 5G желіні құрудың мақсаты болып табылады.

Пайдаланушылардың құпиялылығы мен қауіпсіздігіне қойылатын жоғары талаптар.

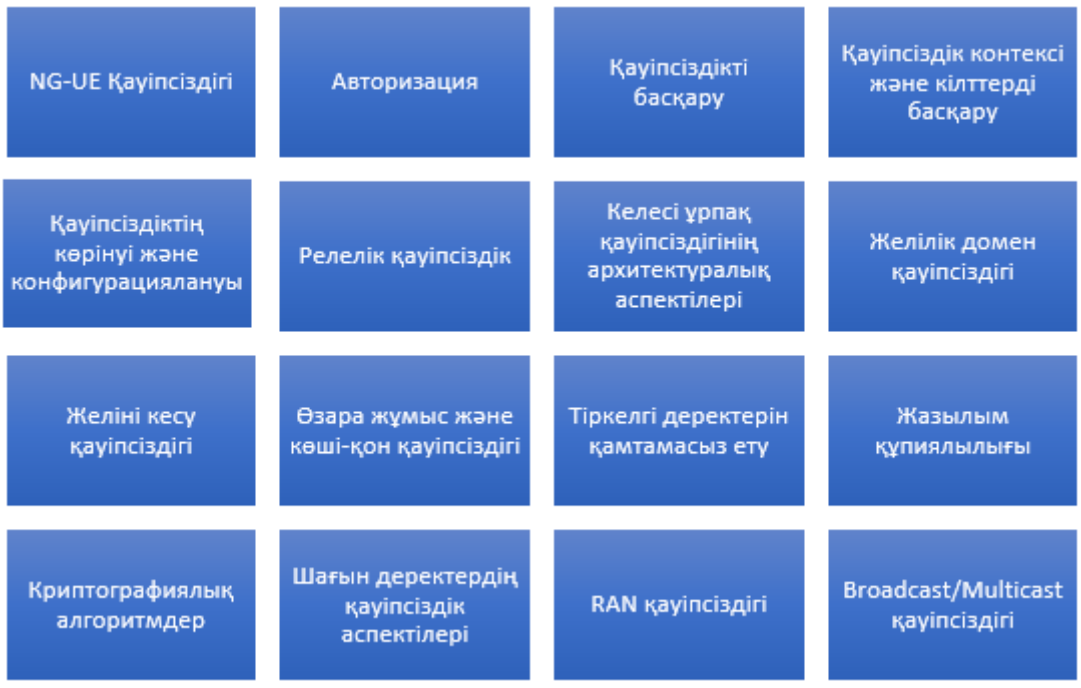
5G пайдаланушылардың құпиялылығын қорғаудың жаңа міндеттерін қойды [2]. Күрделі экожүйе ретінде 5G желісінде: инфрақұрылым жеткізушілері, ұялы байланыс операторлары, виртуалды операторлар және т.б. сияқты бірнеше мүше түрлері бар. Пайдаланушы деректері көптеген қатынас технологияларынан, көп деңгейлі желілерден, бірнеше сақтау құрылғыларынан, берілістерден және өңдеуден тұрады, бірнеше қатысушылар өзара әрекеттесетін күрделі желіде пайдаланушылардың құпиялылық деректерін желінің барлық бұрыштарына шашыратуға болады. Сонымен қатар, 5G желісіне көптеген виртуализация технологиялары енгізілді, бұл икемділікті қамтамасыз етеді және желілік қауіпсіздік шекараларын бұлдыр етеді. Есептеу ресурстарын көп пайдаланушымен бөлісу жағдайында пайдаланушылардың жеке деректері шабуылдар мен жайылып кетулерге осал болады.

Сондай-ақ, 5G желісі құпия мазмұнды артығымен қамтиды және неғұрлым сезімтал. Пайдаланушының жеке өміріне қатысты барлық деректерді (жеке ақпарат, орналасқан жері, орналасқан жері, байланыс мазмұны, байланыс әрекеті, тіркелгі нөмірі және т. б.) қосудан басқа дәстүрлі желілерде қолданылатын, сонымен қатар әр түрлі салаларда жеке адамдар қолданатын жеке мәліметтер (медициналық ақпарат, Қызмет түрлері, қызмет мазмұны және т.б.) және салалық пайдаланушылардың жеке деректері (мысалы, құрылғыны басқару, өндірісті басқару және т. б.) қосылды.

5G жалпы қауіпсіздік архитектурасы.

Осылайша, 5G жаңа қосымшалар сценарийлері, жаңа желілік архитектура, қолданыстағы 4G желісінде қолданылатындардан түбегейлі ерекшеленетін жаңа радио интерфейс технологиялары үшін айтарлықтай қауіпсіздік деңгейін талап етеді. Атап айтқанда, қауіпсіздік жаппай жабдықты аутентификациялау, жоғары қол жетімділікті қамтамасыз ету, төмен кідіріс, төмен қуат тұтыну және IoT Қосымшаларының сценарийлері енгізген басқа да өзгерістер үшін қажет. SDN / NFV, виртуализация, мобильді перифериялық есептеу және басқа да жаңа технологияларды енгізу белгілі бір өзгерістер мен қауіпсіздікке қауіп төндіреді. Алайда, қолданыстағы 4G желілік қауіпсіздік архитектурасы және қауіпсіздіктің негізгі технологиялары 5G қауіпсіздік архитектурасын жобалаудың жаңа мәселелерін шеше алмайды, бұл бірнеше қосымшалар мен жаңа технологиялардың сценарийлерінен туындаған қауіпсіздік мәселелерін шешуге ғана емес, сонымен қатар, әртүрлі сценарийлер үшін сараланған қауіпсіздік тетіктерін қамтамасыз етуге қатысты. 5G қауіпсіздік архитектурасы бірнеше қолданбалы сценарийлерді қолдауы керек және аутентификацияның бірыңғай құрылымын, қызметтерді сертификаттауды, желі сегментінің қауіпсіздігін және пайдаланушының жеке өмірін қорғауды қамтуы керек. Сонымен қатар, әртүрлі қызметтерге сараланған қауіпсіздік қызметтерін ұсыну үшін қауіпсіздік мүмкіндіктерінің даналары икемді түрде іске қосылуы және аяқталуы керек.

3GPP жұмыс тобы, SA 3, 5G желілік қауіпсіздік архитектурасын жобалауға жауап береді және қауіпсіздік архитектурасын жобалау 1-суретте көрсетілген аймақтарды ескеруі керек деп анықтады [2].



Сурет 1. Қауіпсіздік аймағы

Осы даму принциптеріне сүйене отырып, 5GPP [7], ETSI, China's Future Mobile Communications Forum, Ericsson (Ericsson), Nokia, Datang Telecom Technology industry Group, Huawei Technologies Co., Ltd., сондай-ақ басқа да шетелдік кәсіпорындар өздерінің қауіпсіздік сәулет жобаларын ұсынды.

Сонымен, жоғарыда келтірілген шешімдер 5G қауіпсіздік архитектурасының функционалды деңгейіне ұқсас; олар негізінен 4G қауіпсіздік архитектурасының функционалды логикалық құрылымына сәйкес келеді. Сондай-ақ, архитектураға қатысты қауіпсіздік мәселелерін шешу үшін шешімдерді ұсыну қажет, сонымен қатар қауіпсіздік шекараларын өзгерту және басқару жазықтығын түзу жазықтықтан бөлу қажет. Сонымен қатар, сегменттелген желіге сәйкес келетін, арнайы және апаттық сценарийлер үшін ресурстар мен масштабталатын интерфейстерді резервтейтін, сонымен қатар үлкен деректердің қауіпсіздігі үшін ескерту және қорғау механизмдерін қамтамасыз ететін икемді қауіпсіздік механизмдерін жасау қажет. Осыған байланысты, 5G қауіпсіздік архитектурасының мүмкіндіктерін қолдану деңгейінде көптеген инновациялық идеялар әлі біріктірілмегенімен, эндогендік қауіпсіздік дамудың маңызды бағытына айналды.

Маңызды 5G қауіпсіздік технологиялары.

5G жалпы қауіпсіздік архитектурасын негізгі қауіпсіздік технологиялары қолдайды. Жаңа 5G бизнес қолданбалары, жаңа желі құрылымдары, радиоинтерфейсінің жаңа технологиялары және пайдаланушының құпиялылығына қойылатын жоғары қауіпсіздік талаптары да негізгі қауіпсіздік технологияларының эволюциясы мен дамуына түрткі болды. 5G eMBB сценарийі AES, SNOW 3G және ZUC сияқты 4G шифрлау алгоритмдеріне сәйкес келеді. Дегенмен, кванттық есептеу технологияларының біртіндеп дамуымен 4G-де 128-биттік кілтті пайдаланатын AES, SNOW 3G және ZUC криптографиялық алгоритмдері қауіпсіздік қатерлеріне тап болады. Осының негізінде 3GPP SA3 5G желілерінде 128 биттік және 256 биттік кілті бар симметриялық криптографиялық алгоритмді пайдалану туралы талқылауды бастады. AES және SNOW 3G 256 биттік кілт ұзындықтарын қолдайды [8].

mIoT сценарийінде құрылғы қамтамасыз ететін шектеулі қауіпсіздік кеңістігіне байланысты AES, SNOW 3G және ZUC сияқты алгоритмдерді тиімді қолдану мүмкін емес және жеңіл алгоритмді енгізу қажет.

Жалпы, көп доменді, әртараптандырылған, толық және жеңіл қауіпсіздік әртүрлі қауіпсіздік шаралары мен технологияларын қажет етеді. Келесі мәліметтер радиоинтерфейсінің физикалық қабатының қауіпсіздік технологиясын, жеңіл шифрлау технологиясын, желі сегментінің қауіпсіздік технологиясын, 5G пайдаланушының құпиялылығын қорғау технологиясын және жаңа 5G сервистік қолданбаларымен, жаңа желі архитектураларымен және радиоинтерфейсінің жаңа технологияларымен тығыз біріктірілген блокчейн технологиясын көрсетеді.

Жеңілдетілген шифрлау.

Заттар интернеті – 5G қолданбасының әдеттегі сценарийі және оның қауіпсіздік мәселелерін елемеуге болмайды және олардың өзіндік сипаттамалары бар. IoT түйіндерінде әдетте шектеулі аппараттық құралдар мен сигналдарды өңдеу мүмкіндіктері, шектеулі жады, ықшамды өлшем және қатты қуат шектеулері болады. Осылайша, IoT түйіндерінде жеңіл қауіпсіз байланыс механизмі қолайлы және жеңіл қауіпсіздік тетіктері сияқты сипаттамаларды ескере отырып жобалануы керек. Дәстүрлі криптография тұрғысынан сақтау, аппараттық ресурстар және есептеу күрделілігі бойынша қолданыстағы шифрлау алгоритмдерінің құрылымын оңтайландыруға немесе топтастыру, реттілік және хэш функциясына негізделген жаңа жеңіл криптографиялық алгоритмді әзірлеуге болады. Осылайша, қауіпсіздік көрсеткіштерін бұзбай, ресурстар мен энергия шығындарын азайтуға болады. Бұған қоса, өлшеуге, қайта құрылымдауға немесе көшіруге болмайтын жаңа қауіпсіздік элементтерін енгізу үшін сымсыз арнаның эндогендік қауіпсіздік қасиетін пайдалануға болады. Біріктірілген қауіпсіздік және коммуникация дизайнымен, әсіресе жаппай қол жеткізу, шағын деректерді тасымалдау және төмен кідіріс сценарийлері үшін байланыс тиімділігін төмендетпей жеңіл қорғанысқа қол жеткізуге болады.

Желіні бөлу қауіпсіздігі.

Желіні бөлу 5G фазасында желі функцияларын виртуалдандыруды қолданудың негізгі ерекшелігі болып табылады [9]. NFV технологиясын пайдалана отырып, 5G желісінің физикалық инфрақұрылымының ресурстарын сахнаның қажеттіліктеріне сәйкес бірнеше тәуелсіз және параллель виртуалды желі сегменттеріне виртуализациялауға болады. Әрбір сегментті бизнес-процестің қажеттіліктеріне және трафик үлгісіне сәйкес желі функциясына теңшеуге және бейімдеуге болады.

NGMN Alliance [10] желіні бөлу технологиясын қабылдағаннан кейін 5G кездесуі мүмкін қауіпсіздік қатерлері мен қауіпсіздік кемшіліктерін талдап, сегмент қауіпсіздігін қамтамасыз ету үшін шешілуі қажет 10 мәселені атады, соның ішінде:

1) сегменттер арасындағы байланысты басқару;

2) желі сегментінің менеджеріне немесе оператор желісіндегі түйіндік (физикалық) платформаларға қарсы еліктеу шабуылдары үшін талап етілетін инстанция уақыты;

3) оператор желісіндегі қабаттардың даналарына еліктеу шабуылдары;

4) Оператор желісіндегі әртүрлі деңгей менеджерлеріне жалған шабуылдар;

5) Әртүрлі деңгейлер арасындағы әртүрлі қауіпсіздік Хаттамалардың немесе стратегиялардың бірге болуы;

6) қызметтік шабуылдардан бас тарту;

7) басқа деңгейлердегі қауіпсіздік ресурстарының сарқылуы;

8) көлденең-қабатты бүйірлік арналы шабуылдар;

9) гибридті орналастыру үлгісі;

10) UE бірнеше қабаттарға қосылған кезде қабаттар арасындағы оқшаулау.

Олардың ішінде бүйірлік арналық шабуыл ең маңызды мәселе болуы мүмкін және бұл қауіпсіздік мәселесін елемеу мүмкін емес. Мұны сынақ арнасының шабуылының екі аспектісін пайдалану арқылы көруге болады. Біріншісі жай виртуалды машинаны оқшаулауға қатысты: кодтың бір виртуалды машинада қалай жұмыс істейтінін бақылау немесе әсер ету шабуылдаушыға кодтың сол жабдықтағы басқа виртуалды машинада қалай жұмыс істейтіні туралы қандай да бір қорытынды жасауға немесе әсер етуге мүмкіндік бермеуі керек. Екіншісі - сезімталдық деңгейлері өте әр түрлі немесе шабуылдаушыларға осалдықтың өте әртүрлі деңгейлері бар бірдей аппараттық қабаттарда бірлесіп орналасудан аулақ болу. Мысалы, жоғары осал қызметке қолдау көрсететін бір қабатты және сол жабдықта қолданбалы деңгей кодын іске қосуды қолдайтын басқа қабатты бірлесіп орналастырудан аулақ болыңыз. Желіні бөлу қауіпсіздігіне қатысты 3GPP [9] орналастыруды зерттеудің екі кезеңіне бөлінеді: бірінші кезең бөлу қауіпсіздігін оқшаулауды, терминалдық қатынасты қауіпсіз бөлуді және сезімтал желі элементтерінің қауіпсіздігін қамтиды; екінші кезең тәуелсіз қауіпсіздікті қамтиды. Қауіпсіздік стратегиясы және деңгейді басқару сияқты негізгі мәселелер. Атап айтқанда, желі сегменттері арасындағы оқшаулаудың қауіпсіздік талаптарын ескере отырып, осы мақсатқа жету үшін кілтке негізделген техникалық шешім ұсынылады. Бір терминал басқару жазықтығының кілтін ортақ пайдалана алады, бірақ әртүрлі деңгейлерде әртүрлі деректер жазықтығы кілттер пайдаланылады [11].

Пайдаланушының құпиялылығын қорғау.

5G құпиялылығын қорғауға қатысты мазмұнды талдау ескеру қажет кем дегенде үш аспектіні көрсетеді: (1) мобильді желілердегі пайдаланушының құпиялылығын деректерді қорғаудың дәстүрлі қабылдаулары (мысалы, жазылушы деректері, орналасқан жері, байланыс мазмұны, байланыс әрекеті, байланыс қатынасы және тіркелгі нөмірі); (2) әртүрлі салалардағы пайдаланушының құпиялылық деректерін қорғау (мысалы, пайдаланушылардың медициналық және денсаулық туралы ақпараты және көлік құралдарының интернетіндегі құпия ақпарат); және (3) сезімтал салалардағы маңызды деректерді қорғау (мысалы, механикалық және өндірістік бақылауға арналған қолмен деректер). Сонымен қатар, құпиялылық деректеріне төнетін қауіптерді ескере отырып, 5G құпиялылығын қорғау тетіктері мен негізгі технологияларының екі аспектілері бойынша зерттеулер жүргізілуі керек: біріншіден, қамтамасыз ету, өзара әрекеттесу және пайдалану рәсімінде құпиялылық деректерінің ағып кетуін болдырмау мәселесі; және екіншіден, сақтау, беру және пайдалану процедуралары кезінде құпия деректерді бұзу, қирату және ұрлыққа қарсы мәселелер.

5G желілерінде әртүрлі пайдаланушылар, желі элементтері, қолданбалар, бизнес сценарийлері және т.б. әртүрлі құпиялылық талаптарын қоя алады. Сондықтан желі құпиялылықты қорғаудың сараланған мүмкіндіктерін қамтамасыз етуі және 5G желісін пайдаланушылардың деректерінің ағып кетуіне жол бермеу мәселесін шешу үшін әртүрлі техникалық шараларды қабылдауы керек. Біріншіден, 5G желісімен байланысты жеке құпиялылықтың коннотациясы мен ауқымы нақты анықталуы керек және жеке ақпаратты және оған қатысты транзакцияларды өңдейтін және сақтайтын желі субъектілері анық анықталуы керек; онда деректерді азайту, қол жеткізуді басқару, анонимдеу сияқты технологиялар шифрлауды қорғауды және пайдаланушы рұқсатын қабылдауы керек [12].

Блокчейн технологиясы.

5G киберкеңістігінде күрделі сипатқа ие көптеген үлкен нысандар бар. Сонымен қатар, желілік Орта күрделі және виртуалды күй мен физикалық күй бір уақытта болады. Сондықтан күрделі динамикалық ортада әртүрлі желілік элементтер арасындағы өзара ақпараттың тұтастығын қалай қорғауға болатындығын анықтау қажет, ал Интерактивті мінез-құлықтан бас тарту 5G желісі үшін үлкен проблема болып табылады. Блокчейн-бұл бастапқы блоктан бастап қазіргі блокчейн блогына дейінгі барлық транзакцияларды жазатын және орталықсыздандыру, өзгермеу, анонимділік және аудит мүмкіндігінің сипаттамаларына ие таратылған мәліметтер базасы. Ол сонымен қатар жоғарыда аталған мәселелердің шешімін ұсына алады [9].

Желіні қорғау.

Қазіргі уақытта 6,8 миллиард мобильді құрылғы қолданылуда және сансыз IoT құрылғылары бар. 5G дамып келе жатқанда, бұл құрылғылар түрлерінің саны, сондай-ақ қызмет провайдерлеріне жасалған шабуылдардың саны мен ауқымы артады. Mirai ботнеті бір сайтты 600 Гбит/с трафикпен шамадан тыс жүктеу үшін 300 000-нан 500 000-ға дейін құрылғыны пайдаланып бір сайтты қиратты. Бұл біз көрген алғашқы жаппай ботнет шабуылдарының бірі болды, бірақ соңғысы емес. Бұрын желіні бұзуға бірнеше минут кеткен шабуылдар жақын арада бірнеше секундты алады. Кәсіпорынның ақпараттық технологиялар мамандары 5G осалдықтары тудыратын жаңа қауіптермен күресуге дайын болуы керек, бірақ қауіпсіздік топтары жалғыз күреспеуі керек. Қызмет провайдерлері өздерінің абоненттерін және олардың желілерін осы жылдам дамып келе жатқан және тез таралатын қауіптерден қалай қорғауға талпвнуы керек.

IEEE 5G World форумының көптеген қатысушылары қызмет провайдерлері IoT құрылғыларын өндірушілерге олардың өнімдерінің дұрыс қорғалуын қамтамасыз етілуіне сенбеуі керек деп сендірді: қызмет провайдерлері өз желілерін және тұтынушыларын қорғау үшін белсенді қадамдар жасауы керек [11].

EE (Ұлыбританияда бірінші болып 5G желісін ендірген провайдер) әлі 5G қатерлерімен күресуді жоспарлап отырғаны туралы тікелей техникалық мәліметтерді бермегенімен, оның және басқа қызмет провайдерлерінің бірнеше нұсқасы бар екендігін баяндады. 220 Гбит/с-қа дейінгі өткізу қабілеттілігі және 256 миллионға дейін бір мезгілде сеанстарды қолдауы бар жоғары өнімді күйді брандмауэрлер 5G желісі арқылы зиянкестерді блоктауға және жоюға көмектеседі.

Сонымен қатар кеңейтілген сервер жүктемесін теңестіру және FPGA негізіндегі икемді трафикті жеделдету (FTA) DCFW мүмкіндіктері үшін процессорды жүктемес бұрын жалпы аномалия шабуылдарын азайтады. Осылайша, осы қызмет провайдерлері пайдаланатын құралдар мен қауіпсіздік топтарын басып алмай, шабуылдарды азайтуға болады.

Қорытынды

Болашақ 5G қауіпсіздік жүйелерінің толық спектрі қажет, олар әртүрлі қолданбалы сценарийлерге, бірнеше қол жеткізу әдістеріне, сараланған желі қызметтеріне және жоғары өнімділікті, жоғары сенімділік пен қолжетімділікті қамтамасыз ететін жаңа желі архитектурасына негізделеді. Жоғары деңгейдегі қауіпсіздік мүмкіндіктерін қамтамасыз етумен қатар, болашақ 5G қауіпсіздігі белгілі қауіпсіздік тәуекелдері мен белгісіз қауіпсіздік қатерлеріне қарсы тұруы керек.

Ішкі қауіпсіздік элементтері желі архитектурасынан және электромагниттік таралу механизмінен алынып, жаңа қорғаныс механизмдері әзірленуі керек. Бұған қоса, 5G-дің жалпы архитектурасын, бизнес-процестерін және алгоритмдерін жобалау кезінде 5G қауіпсіздік талаптары ескерілсе, біз қауіпсіз және сенімді 5G эндогендік қауіпсіздік желісін құру мақсатына жақындай түсеміз.

Пайдаланылған әдебиеттер тізімі:

1 Толегенова А. С., Айтжанова Н. Т., Казиева Н. М., Тұңғышбайұлы К., Қазақстанда 5g ұялы байланысты енгізу мүмкіндіктерін зерттеу, Вестник науки Казахского агротехнического университета им. С. Сейфуллина (междисциплинарный). – 2015. - №2 (85). – Б.144-149

2 3GPP SA. 3rd generation partnership project service and system aspects. http://www.3gpp.org/specificationsgroups/

3 Analysis of 5G Specification Security and Protocol Vulnerability (Part 1). http://mobile.iotworld.com/View.aspx/News-6ef9a81d4bc5befb

4 NGMN. NGMN 5G white paper. http://ngmn.org/5g-white-paper.html

5 Tolegenova A.S., Zhanys A.B., Nurkasymova S.N., Soboleva L.A., Overview of 4G, 5G radio spectrum in the world and Kazakhstan, Advances in Composite Science and Technology (ACST 2019), IOP Conf. Series: Materials Science and Engineering 934 (2020) 012055

6 3GPP. 3rd generation partnership project; technical specification group services and system aspects; study on the security aspects of the next generation system (Release 14). TR 33.899 version 1.3.0, 2017

7 5GPP. 5G PPP phase1 security landscape produced by the 5G PPP security WG. 2017. https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf

8 John Mattsson, 5G Encryption. SAAG, IETF 104 Prague, March 2019, Ericsson

9 Amir Afaq, Noman Haider, Muhammad Zeeshan Baig, Komal S. Khan, Muhammad Imran, Imran Razzak, Machine learning for 5G security: Architecture, recent advances, and challenges, Ad Hoc Networks, Volume 123, 2021, 102667,ISSN 1570-8705

10 *ETSI. Network function virtualization: architectural framework. 2017 https://www.etsi.org/deliver/etsi_gr/nfv/001_099/001/01.02.01_60/gr_nfv001v010201p.pdf*

11 IEEE 5G World Forum, home page.Accessed Oct 2018. http://ieee-wf-5g.org.

12 El-Moghazi, Mohamed and Whalley, Jason, IMT-2020 Standardization: Lessons from 5G and Future Perspectives for 6G (August 7, 2021). Available at SSRN: https://ssrn.com/abstract=3901148 or http://dx.doi.org/10.2139/ssrn.3901148

References:

1 Tolegenova A.S., Ajtzhanova N.T., Kazieva N.M., Tungyshbajuly K., (2015) Kazakstanda 5g ujaly bajlanysty engizu mumkindikterin zertteu [Study of the possibility of implementing 5g mobile communication in Kazakhstan]. Vestnik nauki Kazahskogo agrotehnicheskogo universiteta im. S. Sejfullina (mezhdisciplinarnyj). №2 (85). 144-149

2 3GPP SA. 3rd generation partnership project service and system aspects. http://www.3gpp.org/specificationsgroups/

3 Analysis of 5G Specification Security and Protocol Vulnerability (Part 1). http://mobile.iotworld.com/View.aspx/News-6ef9a81d4bc5befb

4 NGMN. NGMN 5G white paper. http://ngmn.org/5g-white-paper.html

5 A S Tolegenova,, A B Zhanys, S N Nurkasymova, L A Soboleva1, Overview of 4G, 5G radio spectrum spectrum in the world and Kazakhstan, Advances in Composite Science and Technology (ACST 2019), IOP Conf. Series: Materials Science and Engineering 934 (2020) 012055

6 3GPP. 3rd generation partnership project; technical specification group services and system aspects; study on the security aspects of the next generation system (Release 14). TR 33.899 version 1.3.0, 2017

7 5GPP. 5G PPP phase1 security landscape produced by the 5G PPP security WG. 2017. https://5g-ppp.eu/ wp-content/uploads/2014/02/5G-PPP WhitePaper Phase-1-Security-Landscape June-2017.pdf

8 John Mattsson, 5G Encryption. SAAG, IETF 104 Prague, March 2019, Ericsson

9 Amir Afaq, Noman Haider, Muhammad Zeeshan Baig, Komal S. Khan, Muhammad Imran, Imran Razzak, Machine learning for 5G security: Architecture, recent advances, and challenges, Ad Hoc Networks, Volume 123, 2021, 102667,ISSN 1570-8705

10 ETSI. Network function virtualization: architectural framework. 2017.https://www.etsi.org/deliver /etsi_gr/nfv/001_099/001/01.02.01_60/gr_nfv001v010201p.pdf

11 IEEE 5G World Forum, home page.Accessed Oct 2018. http://ieee-wf-5g.org.

12 El-Moghazi, Mohamed and Whalley, Jason, IMT-2020 Standardization: Lessons from 5G and Future Perspectives for 6G (August 7, 2021). Available at SSRN: https://ssrn.com/abstract=3901148 or http://dx.doi.org/10.2139/ssrn.3901148