ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті» коммерциялық емес акционерлік қоғамы

Автоматика және ақпараттық технологиялар институты

Электроника, телекоммуникация және ғарыштық технологиялар кафедрасы

Джахметов Асанәлі Ерланұлы

«IoT технологиясындағы үзіліссіз байланыс механизмінің қауіпсіздігін зерттеу»

ДИПЛОМДЫҚ ЖҰМЫС

6В06201 – «Телекоммуникация»

Алматы 2024

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті» коммерциялық емес акционерлік қоғамы

Автоматика және ақпараттық технологиялар институты

Электроника, телекоммуникация және ғарыштық технологиялар кафедрасы

ҚОРҒАУҒА ЖІБЕРІЛДІ
Кафедра меңгерушісі
техн.ғыл.канд.
_____Е.Таштай
«29» 05 2024 ж.

ДИПЛОМДЫҚ ЖҰМЫС

Тақырыбы «IoT технологиясындағы үзіліссіз байланыс механизмінің қауіпсіздігін зерттеу»

6В06201 – «Телекоммуникация»

Орындаған: Джахметов А.Е

Пікір беруші:
ҚазҰАЗУ PhD,
қауымдастырылған профессор
_____ Әлібек Н.
«28» 05 2024 ж.

Ғылыми жетекші
PhD,ЭТжҒТ,
қауымдастырылған профессор
_____ Тайсариева К.Н
«29» 05 2024 ж.

Алматы 2024

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Автоматика және ақпараттық технологиялар институты

Электроника, телекоммуникация және ғарыштық технологиялар кафедрасы

6В06201 Телекоммуникация

БЕКІТЕМІН
Кафедра меңгерушісі
_____ Е. Таштай
«_19_» ___1___ 2023 ж.

Дипломдық жұмыс орындауға
ТАПСЫРМА

Білім алушы Джахметов Асанәлі Ерланұлы

Тақырыбы «IoT технологиясындағы үзіліссіз байланыс механизмінің қауіпсіздігін зерттеу»

Университет ректорының *«4» 12 2023 ж. №548-П/Ө бұйрығымен бекітілген.*

Аяқталған жұмысты тапсыру мерзімі *« 30 » 04 2024 ж.*

Дипломдық жұмыстың бастапқы берілістері:

1) Заттардың қауіпсіз интернетінің тұжырымдамасы, IoT негіздерін қарастыру;
2) IoT негізіндегі смарт жүйесін құру және енгізу: WPA/WPA2 қауіпсіздік және RADIUS серверін пайдалану;
3) IoT үшін аппараттық және қосылу технологияларын талдау: қауіпсіздікті, қолданбаларды және коммуникацияларды бағалау;
4) IoT бағдарламалық қамтамасыз ету желісінің қауіпсіздігін, деректерді қорғау үшін заманауи протоколдар мен құралдарды зерттеу.

Дипломдық жұмыста қарастырылатын мәселелер тізімі:

1) Байланыс қауіпсіздігін қамтамасыз ету үшін IoT протоколдары мен стандарттарын (WPA, WPA2) зерттеу.
2) Смарт желісінің инфрақұрылымын конфигурациялау және қауіпсіздік сынағы;
3) CISCO Packet Tracer бағдарламасында Байланыс қауіпсіздігін қамтамасыз ету үшін IoT технологиясының WPA немесе WPA2 сияқты протоколдарын қолдану;
4) Wireshark бағдарламасы арқылы желілік трафикті талдау және байланыс хаттамаларын, пайдаланушыға нақты уақыт режимінде желі арқылы өтетін барлық трафикті зерттеу.

Сызбалық материалдар тізімі (міндетті сызбалар дәл көрсетілуі тиіс):

Ұсынылатын негізгі әдебиеттер:

1) Abdellah A.R. Deep Learning for IoT Traffic Prediction Based on Edge Computing. /
Abdellah A.R., Artem V., Muthanna A., Gallyamov D., Koucheryavy A. // In: Vishnevskiy V.M., Samouylov K.E., Kozyrev D.V. (eds) Distributed Computer and Communication Networks: Control, Computation, Communications. DCCN 2020. Communications in Computer and Information Science. Springer,
2)Ali R. Abdellah, "IoT traffic prediction using multi-step ahead prediction with neural network," /Ali R. Abdellah, Omar Abdul Kareem Mahmood, Alexander Paramonov, Andrey Koucheryavy // 2019 11th International Congress on Ultra Modern 140 Telecommunications and Control Systems and Workshops (ICUMT), Dublin, Ireland, 2019, pp. 1-4

Дипломдық жұмысты (жобаны) дайындау
КЕСТЕСІ

Бөлімдер атауы, қарастырылатын мәселелер тізімі	Ғылыми жетекшіге және кеңесшілерге көрсету мерзімі	Ескерту
Заттардың қауіпсіз интернетінің тұжырымдамасы, IoT негіздері және күрделілігі.	04.01.2024 - 01.02.2024	Орындалды
CISCO Packet Tracer бағдарламасында байланыс қауіпсіздігін қамтамасыз ету үшін IoT стандарттары мен WPA, WPA2 протоколдарын қолдану.	01.02.2024 - 01.03.2024	Орындалды
Wireshark бағдарламасы арқылы желілік трафикті талдау және байланыс хаттамаларын,пайдаланушыға нақты уақыт режимінде желі арқылы өтетін барлық трафикті зерттеу.	01.03.2024- 30.05.2024	Орындалды

Дипломдық жұмыс (жоба) бөлімдерінің кеңесшілері мен норма бақылаушының аяқталған жұмысқа(жобаға) қойған **қолтаңбалары**

Бөлімдер атауы	Кеңесшілер (аты, әкесінің аты, тегі, ғылымидәрежесі, атағы)	Қол қойылған күні	Қолы
Диплом жұмысының тақырыбын талдау	Тайсариева К.Н., PhD., ЭТжҒТ, қауымдастырылған профессор	04.11.2023	
Теориялық ақпарат	Тайсариева К.Н., PhD., ЭТжҒТ қауымдастырылған профессор	20.05.2024	
Норма бақылау	Досбаев Ж.М. ЭТжҒТ, PhD., аға оқытушысы	28.05.2024	

Ғылыми жетекшісі Тайсариева К.Н.

Тапсырманы орындауға алған білім алушы Джахметов А.Е

Күні «8»12 2023ж.

АҢДАТПА

Бұл зерттеу WPA/WPA2 протоколдарын және RADIUS сервері арқылы орталықтандырылған аутентификацияны қолдану арқылы қауіпсіздікті қамтамасыз етуге баса назар аудара отырып, Интернет заттары (IoT) технологиясындағы үздіксіз байланыс механизмінің қауіпсіздігін зерттеудің өзекті тақырыбына арналған. Киберқауіпсіздік қатерлерінің көбеюіне байланысты бұл зерттеу жеке деректерді қорғау және құрылғыларға қол жеткізуді бақылау қажеттілігіне бағытталған. Зерттеуге IoT аппараттық және бағдарламалық аспектілерін талдау, желі архитектурасын және құрылғылардың қауіпсіз өзара әрекеттесуін енгізу кіреді.

Жұмыстың мақсаты – кибер-кеңістіктегі заманауи қауіптерге төтеп бере алатын ауқымды және қауіпсіз жүйені әзірлеу. Осы мақсатқа жету үшін Wireshark бағдарламасы арқылы желілік трафикті түсіру және талдау, Cisco Packet Tracer жүйесінде желілік инфрақұрылымды модельдеу және әртүрлі шабуыл сценарийлері мен қорғаныс әдістерін қолдану арқылы жүйені сынау үшін пайдаланылды.

Жұмыстың нәтижелері қазіргі заманғы қауіпсіздік хаттамалары мен орталықтандырылған аутентификация әдістерін біріктіру жүйелердің қауіпсіздік деңгейін айтарлықтай арттыруға болатындығын көрсетеді. Жүйені енгізу, одан кейінгі тестілеу оның қол жеткізуді тиімді басқару және пайдаланушы деректерін қорғау қабілетін көрсетті. Жұмыс жеке үй шаруашылығында, өнеркәсіптік ауқымда да қолдануға болатын IoT қауіпсіздігін жақсарту бойынша құнды қорытындылар мен ұсыныстарды береді, бұл оны технологияның дамуының қазіргі кезеңінде өзекті және сұранысқа ие етеді.

АННОТАЦИЯ

Дипломная работа посвящена актуальной теме исследования безопасности механизма бесперебойной связи в технологии Интернета вещей (IoT), с акцентом на обеспечении безопасности с использованием протоколов WPA/WPA2 и централизованной аутентификации через RADIUS-сервер. В свете растущего числа угроз кибербезопасности, работа акцентирует внимание на необходимости защиты личных данных и управления доступом к устройствам. Исследование включает анализ аппаратных и программных аспектов IoT, сетевой архитектуры и реализацию безопасного взаимодействия устройств.

Цель работы — разработать масштабируемую и защищённую систему, способную противостоять современным угрозам в киберпространстве. Для достижения этой цели были использованы программы Wireshark, для достижения захвата и анализа трафика сети, моделирование сетевой инфраструктуры в Cisco Packet Tracer и тестирование системы с использованием различных сценариев атак и методов защиты.

Результаты работы демонстрируют, как интеграция современных протоколов безопасности и централизованных методов аутентификации может

значительно повысить уровень защиты систем. Реализация и последующее тестирование системы показали её способность эффективно управлять доступом и защищать данные пользователей. Работа предоставляет ценные выводы и рекомендации по улучшению безопасности IoT, которые могут быть применены как в частных домохозяйствах, так и в промышленных масштабах, что делает её актуальной и востребованной на современном этапе развития технологий.

ABSTRACT

This study is devoted to the current topic of research into the security of the uninterrupted communication mechanism in Internet of Things (IoT) technology, with an emphasis on ensuring security using the WPA/WPA2 protocols and centralized authentication through a RADIUS server. In light of the growing number of cybersecurity threats, the work focuses on the need to protect personal data and control access to devices. The research includes analysis of hardware and software aspects of IoT, network architecture and implementation of secure device interaction.

The goal of the work is to develop a scalable and secure system that can withstand modern threats in cyberspace. To achieve this goal, Wireshark programs were used to capture and analyze network traffic, simulate the network infrastructure in Cisco Packet Tracer and test the system using various attack scenarios and defense methods.

The results of the work demonstrate how the integration of modern security protocols and centralized authentication methods can significantly increase the level of security of systems. The implementation and subsequent testing of the system showed its ability to effectively manage access and protect user data. The work provides valuable conclusions and recommendations for improving IoT security, which can be applied both in private households and on an industrial scale, which makes it relevant and in demand at the present stage of technology development.

МАЗМҰНЫ

КІРІСПЕ

Интернет заттары (IoT) – құрылғылардың, қоршаған ортаның және адамдардың өзара әрекеттесу тәсілін өзгертетін озық технология. Цифрлық технологиялар өмірдің әртүрлі салаларында маңыздырақ бола бастаған уақытта IoT смарт жүйелерді құруда, тиімділік пен жайлылық деңгейін арттыруда, сондай-ақ ресурстар мен қоршаған ортаны басқаруда маңызды рөл атқарады.

IoT идеясын алғаш рет 1999 жылы Кевин Эштон ұсынды, ол тұжырымдаманы адамның тікелей араласуынсыз Интернет арқылы деректер алмасуға қабілетті құрылғылар желісі ретінде сипаттады. Дегенмен, IoT негіздері автоматтандыру және сымсыз байланыс желілеріндегі бұрынғы зерттеулерде жатыр.

IoT дамуы микроэлектроникадағы, құрамдас бөліктерді миниатюризациялаудағы және сымсыз байланыс технологияларын дамытудағы елеулі жетістіктердің арқасында мүмкін болды. Бұл ықшам, энергияны үнемдейтін және қолжетімді құрылғыларды жасауға мүмкіндік берді, бұл олардың өмір мен өндірістің әртүрлі салаларында кеңінен қолданылуына ықпал етті.

IoT технологиясы бүкіл әлемде өмір мен өнеркәсіптің әртүрлі салаларында қолданыла бастады. Медицинада ол пациенттердің жағдайын бақылау, медициналық деректерді жинау, талдау және медициналық жабдықты басқару үшін қолданылады. Ақылды қалаларда IoT көлік инфрақұрылымын басқару, ресурстарды пайдалануды оңтайландыру және азаматтардың қауіпсіздігін қамтамасыз ету үшін қолданылады. Өнеркәсіпте IoT өндірістік процестерді бақылау және ресурстарды пайдалануды оңтайландыру, сонымен қатар өндіріс тиімділігін арттыру үшін қолданылады.

Құрылғылар Wi-Fi, Bluetooth, Zigbee, LoRa және NB-IoT сияқты әртүрлі протоколдар мен коммуникациялық технологияларды пайдалана отырып, IoT жүйесінде байланысады. Бұл құрылғыларға нақты уақытта да, кідіріспен де ақпарат алмасуға, жергілікті немесе орталық серверлерде деректерді өңдеуді жүзеге асыруға мүмкіндік береді.

Заттар интернеті құрылғыларды, деректерді және адамдарды бір сандық экожүйеге біріктіретін әлеміміздің ажырамас бөлігіне айналуда. Қосылған құрылғылар санының артуымен IoT өмір сүру сапасын жақсартуға және қызметтің әртүрлі салаларында тиімділікті арттыруға жаңа мүмкіндіктер ашатын дамуды жалғастыруда.

Бұл зерттеуде біз IoT технологиясының негіздері мен қауіпсіздігін талдауға, оның қазіргі цифрлық әлемдегі негізгі аспектілері мен маңыздылығын анықтауға назар аударамыз.

Зерттеуіміздің бірінші бөлімінде біз Интернет заттар технологиясының жұмыс істеу негіздерін және оның қауіпсіздік принциптерін егжей-тегжейлі қарастырамыз. Деректерді және пайдаланушының құпиялылығын қорғау үшін IoT қауіпсіздігінің маңыздылығына ерекше назар аударылады. Біз сондай-ақ IoT желілері кездесетін әртүрлі қауіпсіздік мәселелерін талдаймыз және IoT

технологиялары контекстінде үздіксіз байланыстың қауіптері мен тәуекелдерін, сондай-ақ коммуникацияларды қорғау әдістерін қарастырамыз.

Келесі, зерттеуіміздің екінші бөлімінде біз IoT желілерінде қолданылатын әртүрлі технологиялар және олардың стандарттары мен механизмдерін зерттейміз. Бұл коммуникациялық технологияларды талдауды, қауіпсіздіктің құрылыс блоктарын, деректер үлгілерін және IoT деректер моделін және жүйе абстракцияларын талдауды қамтиды.

Зерттеуіміздің қорытынды бөлімінде IoT желілеріндегі қауіпсіз байланысты қамтамасыз ету үшін біз IoT стандарттары мен WPA немесе WPA2 сияқты протоклдарын пайдалана отырып, өзара әрекеттестікке талдау жасаймыз. Сонымен қатар, біз CISCO Packet Tracer және Wireshark бағдарламаларының көмегімен желілік трафикті және байланыс протоколдарын талдауды, трафикті нақты уақытта тексеруді қарастырамыз.

Дегенмен, IoT технологиясының мүмкіндіктерімен қатар қауіпсіздік пен деректердің құпиялылығы мәселелерін қоса алғанда, қиындықтар туындайды. Ақпаратты қорғау және желі қауіпсіздігін қамтамасыз ету осы технологияны қолданудың маңызды аспектісі. Сондай-ақ, IoT инновациялар үшін жаңа көкжиектер ашатын және өмір сүру сапасын жақсартатын цифрлық трансформацияның негізгі құрамдас бөлігі болып табылатынын, бірақ сонымен бірге деректер қауіпсіздігі мен құпиялылық мәселелеріне назар аударуды талап ететінін ескеру керек.

1 IoT технологиясы

Интернет заттары деректер желісіне қосылу құралдарымен міндетті түрде жабдықталмаған физикалық объектілерді пайдаланады, сондықтан осы объектілерді («заттарды») сәйкестендіру үшін технологияларды пайдалануды талап етеді RFID (Radio Frequency Identification – Радиожиілік идентификациясы) осы тұжырымдаманың бастамашысы, бірақ оптикалық танылған идентификаторлар. (штрих-кодтар) мұндай технология ретінде пайдаланылуы мүмкін, кодтар, QR кодтары), нақты уақыттағы орынды анықтау құралдары және автоматты сәйкестендірудің кез келген басқа құралдары осындай технология ретінде пайдаланылуы мүмкін. Заттар интернетінің кеңінен таралуына байланысты стандарттауды талап ететін объект идентификаторларының бірегейлігін қамтамасыз ету өте маңызды.

Интернетке тікелей қосылған объектілер жағдайында дәстүрлі идентификатор желілік адаптердің MAC мекенжайы болып табылады, ол құрылғыны деректер байланысы деңгейінде сәйкестендіруге мүмкіндік береді, алайда қол жетімді мекенжайлар ауқымы іс жүзінде сарқылмайды (2^48). MAC-48 кеңістігіндегі мекенжайлар) және IPv6 хаттамасы планетаның әрбір тұрғыны үшін кемінде 300 миллион құрылғы үшін бірегей мекенжайлар желісінің деңгейін қамтамасыз етеді, бұл мұндай құрылғыларды анықтауға кең мүмкіндіктер береді.

Заттар интернетінде өлшеу құралдары ерекше рөл атқарады және сыртқы орта туралы ақпаратты машина оқитын деректерге түрлендіре отырып, есептеу ортасын мағыналы ақпаратпен толтыруға мүмкіндік береді. Қарапайым датчиктерден (мысалы, температура, қысым, жарық) және өлшеу құрылғыларынан (мысалы, смарт есептегіштер) күрделі біріктірілген өлшеу жүйелеріне дейін өлшеу құралдарының кең ауқымы қолданылады. «Заттардың интернеті» концепциясы шеңберінде өлшеу құрылғыларын желілерге біріктіру (мысалы, сымсыз сенсорлық желілер, өлшеу жүйелері) іргелі болып табылады, бұл машинадан машинаға байланыс жүйелерін құруға мүмкіндік береді.

Заттар интернетін жүзеге асырудағы ерекше практикалық мәселе – өлшеу құралдарының максималды автономиясын қамтамасыз ету қажеттілігі, бұл бірінші кезекте сенсорларды электрмен жабдықтау мәселесін көрсетеді. Сенсорларды автономды электрмен жабдықтауды қамтамасыз ететін тиімді шешімдерді табу (фотоэлементтерді пайдалану, дірілден энергияны түрлендіру, ауа ағындары және электр энергиясын сымсыз беру), техникалық қызмет көрсету шығындарын арттырмай (батареяларды ауыстыру немесе сенсорлық батареяларды зарядтау түрінде), сенсор желілерін кеңейтуге болады.

Мәліметтерді жіберудің ықтимал технологияларының ауқымы сымсыз және сымды желілердің барлық мүмкін құралдарын қамтиды.

Сымсыз деректерді беруде төмен жылдамдықтағы тиімділік, ақауларға төзімділік, бейімделу және өзін-өзі ұйымдастыру сияқты қасиеттер заттар интернетін құруда ерекше маңызды рөл атқарады. IEEE 802.15.4 стандарты физикалық деңгейді және энергияны конфигурациялау үшін қол жеткізуді

басқаруды анықтайды. Тиімді жеке аймақтық желілер және ZigBee, WirelessHart, MiWi, 6LoWPAN және LPWAN сияқты хаттамалардың негізі болып табылады.

Сымды технологиялар арасында PLC (Power line communication – дауыс немесе деректер ақпаратын беру үшін электр желілерін (электр желілерін) пайдаланудың бірнеше әртүрлі жүйелерін сипаттайтын термин. Желі аналогты сигналды стандартты 50 Гц немесе 60 Гц айнымалы ток қуатының үстіне қою арқылы дауыс пен деректерді тасымалдай алады.) шешімдері Интернет заттарының таралуында маңызды рөл атқарады. Себебі көптеген қолданбалар электр желісіне қол жеткізеді (мысалы, сауда автоматтары, банкоматтар, смарт есептегіштер және жарықтандыру контроллері алдымен электр желісіне қосылады). 6LoWPAN IEEE 802.15.4 және PLC үшін IPv6 деңгейін жүзеге асырады және IETF (Internet Engineering Task Force, Интернет-инженерлік жұмыс тобы – бұл 1986 жылы IAB (Internet Architecture Board-Интернет-архитектура кеңесі) құрған, интернет хаттамалары мен архитектурасын дамытуға арналған дизайнерлердің, ғалымдардың, желі операторлары мен провайдерлерінің ашық халықаралық қауымдастығы) стандартымен стандартталған. Бұл IETF стандартталған ашық хаттама және заттар интернетін дамыту үшін ерекше маңызды деп танылған[1].

1.1 IoT қосылуының негіздерін және қауіпсіздігін талдау

Интернет заттарына қосылған құрылғылар сенсорлар, микробағдарлама және қатысты технологиялар сияқты физикалық нысандар және басқа жүйелер мен құрылғылар арасында деректер алмасатын әлемді жасайды. Бұл алмасуға мүмкіндік беретін негізгі технология – заттар интернетіндегі «заттар» арасындағы байланыс. Құн тізбегі бойынша орасан зор құн жасалуда, өйткені ұйымдар жаңа мүмкіндіктерді, жаңа бизнес үлгілерін және IoT байланысы арқылы жаңа кірістерді қабылдайды.

IoT құрылғыларының талаптарына байланысты IoT қосылымының әртүрлі түрлері қолданылады: IoT құрылғыларынан және шағын деректер көлемімен жиі байланысты қажет ететін қосылған құрылғылардан бастап, үлкен көлемдегі деректерді жоғары жылдамдықпен тасымалдауды қажет ететін әрқашан қосылған IoT құрылғыларына дейін және төмен кідіріс.. Интернетке тіс имплантаты сияқты кішкентай нәрседен бастап трактор сияқты үлкен нәрсеге дейін әртүрлі нысандарды қосуға болады.

Осы әртүрлі нәрселердің барлығын IoT-ке қосу және оларға сенсорларды қосу цифрлық интеллекттің жаңа деңгейіне әкеледі, бұл қосылған құрылғыларға нақты уақыт режимінде байланысуға және кең ауқымды автоматтандыру процестеріне қатысуға мүмкіндік береді. Заттар интернеті жетілген сайын қосылымдар саны жылдам өсуде және IoT қосылған құрылғылар санына арналған болжамдар Интернетке қосылған құрылғылардың үлкен санын орналастырудың өсу үрдісін көрсетеді.

Қазіргі уақытта шамамен 14 миллиард IoT қосылған құрылғылар бар, бұл смартфондар, планшеттер, дербес компьютерлер және қалалық телефондар сияқты IoT-қа қосылмаған құрылғылардың санынан асып түседі. Бұл сан 2025 жылға қарай 30 миллиард құрылғыға дейін өседі деп күтілуде, өйткені заттар интернеті айналамыздағы әлемді одан да интеллектуалды және икемді етеді, цифрлық және физикалық ғаламдар біріктіреді.

Қосылған IoT құрылғыларының түрлері шамдарды қосу және өшіру немесе қоқыс жәшігі толған кезде билік органдарына хабарлау сияқты салыстырмалы түрде қарапайым функцияларды орындайтын сенсорлар мен жетектерден бастап, көлікті ортақ пайдалану жүйесі сияқты күрделі, әрқашан қосылатын құрылғыларға дейін ауытқиды. Үздіксіз мониторинг, мысалы, үздіксіз суық тізбек логистикасын қамтамасыз етудегі өзінің құндылығын дәлелдеді, бірақ тіпті жаңа қолданбалар телемедицина процедуралары және бейнеге негізделген қауіпсіздік сияқты пайдалану жағдайларын қосу үшін жоғары өткізу қабілеті мен төмен кідіріс қосылымына байланысты болады.

2025 жылға қарай заттар интернетіне қосылған ондаған миллиард құрылғылармен пайдалану жағдайларының саны да тез өсіп, заттар интернетін жаңа нарықтарға шығарады. Сонымен қатар, IoT құрылғыларының әртүрлі қажеттіліктерін қанағаттандыру үшін қосылу әдістері әртараптандырылуда. Ұялы байланыс нарығы 1G-ден 5G-ге көшті, мұнда 5G ұялы байланыстың алдыңғы буындарымен бірге ультра жоғары жылдамдықты, өте төмен кідірісті және халық тығыз орналасқан аудандарға көптеген IoT құрылғыларын қосу мүмкіндігін қажет ететін қосылымға мүмкіндік береді.

IoT қосылымының әртүрлі түрлері бар және IoT құрылғысының әрбір түрі оңтайлы шешімге ие болуы мүмкін. Ол қамту аймағына негізделген қолданбаларға, жүйелерге, бағдарламалық құралға және қосылуды қажет ететін құрылғыларға арналған IoT құрылғысының талаптарына сәйкес келеді. Әр түрлі қосылымдар мен құрылғылар біріктіріліп, инновацияларды басқарып, құрылғыларды қосу және цифрлық және физикалық әлемдерді қосу арқылы қол жеткізуге болатын жетістіктердің ауқымын кеңейте отырып, гипер масштабты заттар интернетін құруда.

Заттардың интернеті өзінің әлеуетін жүзеге асыру үшін бірнеше сымсыз технологияларды пайдалану қажет. Мысалы, Bluetooth Low Energy және IEEE 802.15.4 батареямен жұмыс істейтін сенсорлар үшін қолайлы, бірақ үнемі қозғалыста немесе жергілікті желіден тыс құрылғылар үшін бұл салыстырмалы түрде қысқа қашықтықтағы сымсыз технологиялар Интернетке қосылу үшін жарамсыз.

Тіпті жергілікті желілермен де, өндірушілер ыңғайлылық пен автономия үшін ұзағырақ диапазондағы сымсыз технологияларды таңдауы мүмкін. Мысалы, құрылғы өндірушілер ұялы Wi-Fi технологиясын таңдай алады, себебі ол тоңазытқыштар мен кір жуғыш машиналарды бұлтқа автоматты түрде қосады, бұл тұтынушылардың үйдегі жергілікті желісіне құрылғылар қосу үшін құпия сөздерді енгізу қажеттілігін болдырмайды. Төмен қуатты кең жолақты желілер

(LPWANs) және тар жолақты заттар интернеті технологиялары бұл жағдайда көмектесе алады.

Қазіргі уақытта IoT әрқайсысының өзіндік бірегей мүмкіндіктері бар көптеген сымсыз желі технологияларын пайдаланады. Сол сымсыз желі технологиялары радиожиіліктерде таралу себебімен олар: лицензиялық және лицензиясыз деп екіге бөлінеді.

Лицензияланған спектрге қолжетімділік әдетте жергілікті билік органдарынан сатып алынады, бұл ұйымға белгілі бір орындағы белгілі бір арнаға эксклюзивті рұқсат береді. Бұл арнадағы жұмыс негізінен бәсекелес радиостанциялардың кедергілерінен таза болуы керек. Кемшіліктері мынада: қамтылған жиілік диапазондары өте кішкентай немесе қол жеткізу қымбат болуы мүмкін. Бұған қоса, бір елде рұқсат етілген спектр жолақтары басқа елде пайдалану үшін қол жетімді болмауы мүмкін. Мысалы, Үндістандағы ұялы желілер 900 МГц және 1800 МГц жолақтарын пайдаланады. АҚШ-тағы мобильді байланыстардың ғаламдық жүйесі (GSM) ұялы байланыс операторлары 850 МГц және 1900 МГц жолақтарын пайдаланады, ал Қазақстанның қалаларында және облыс орталықтарының көпшілігінде GSM жиілігі 1710-1880 МГц, ауылдық жерлерде 890-960 МГц қолданылады. IoT құрылғыларын жаһандық орналастыру бірнеше радио диапазондарын қолдауды талап етеді, бұл құрылғыларды қымбаттатады және әзірлеу уақытын қажет етеді. Лицензияланған жолақтар жылдам орналастыруға жарамайды, себебі спектр оңай қол жетімді болса да операциялық лицензияны алу бірнеше айға созылуы мүмкін. Лицензиясыз спектр жұртшылық үшін ашық және оны кез келген адам пайдалана алады, нақты ұйымдарға немесе жеке тұлғаларға ерекше құқықтар бермей. Кемшілігі - бәсекелес жүйелер әртүрлі қуат деңгейлерінде бір арнаны алып, кедергілерге әкелуі мүмкін. Лицензиясыз диапазонда жұмыс істейтін радиожүйелерді өндірушілер осы ықтимал кедергіге жұмысын бейімдеу үшін радио құрылғыларына мүмкіндіктер енгізді. Бұл технологияларға адаптивті модуляция, беріліс қуатын автоматты басқару және диапазоннан тыс сүзу кіреді.

IoT қауіпсіздігін талдау – бұл осалдықтарды анықтау және оларды жою немесе азайту шараларын әзірлеу үшін құрылғыларды, желілерді және қолданбаларды қоса алғанда, заттар интернеті (IoT) жүйелерінің қауіпсіздік жағдайын зерттеу және бағалау процесі. Оған бірнеше қадамдар кіреді:

Құрылғы мен құрамдас идентификация: IoT жүйесін құрайтын барлық құрылғыларды, сенсорларды, контроллерлерді, желілік құрылғыларды және басқа компоненттерді анықтау.

Қауіпсіздікті бағалау: әрбір құрылғы мен құрамдас үшін қауіпсіздіктің ағымдағы деңгейін бағалау, соның ішінде бағдарламалық жасақтаманың соңғы жаңартуларының қолжетімділігін, күшті аутентификация және деректерді шифрлау әдістерінің бар болуын және мониторинг пен аномалияны анықтау механизмдерінің бар болуын қамтамасыз ету.

Ықтимал осалдықтарды анықтау: бағдарламалық жасақтамадағы, қауіпсіздік параметрлеріндегі, физикалық қауіпсіздіктегі және шабуылдаушылар

пайдалануы мүмкін басқа аспектілердегі ықтимал осалдықтарды анықтау үшін жүйені талдайды.

Тәуекелді бағалау: әрбір осалдықты пайдаланудың ықтималдығы мен ықтимал әсерін бағалау. Бұл ықтимал қауіптерді және олардың деректердің және тұтастай алғанда жүйенің құпиялылығына, тұтастығына, қолжетімділігіне әсерін талдауды қамтиды.

Қауіпсіздік стратегиясын әзірлеу: Талдау нәтижелеріне сүйене отырып, осалдықтарды жою, қосымша қауіпсіздік басқару элементтерін енгізу және қауіпсіздікті басқару процестерін жақсарту бойынша ұсыныстары бар қауіпсіздік стратегиясын жасаңыз.

Қауіпсіздік шараларын іске асыру: Қауіпсіздік стратегиясы әзірленгеннен кейін бағдарламалық құралды жаңарту, қауіпсіздік параметрлерін өзгерту, жаңа қауіпсіздік механизмдерін қосу және қызметкерлерді оқыту сияқты ұсынылған қауіпсіздік шаралары орындалады.

Бақылау және жаңарту: Қауіпсіздік шаралары енгізілгеннен кейін IoT жүйелері олардың қауіпсіздігін уақыт өте келе қамтамасыз ету үшін үздіксіз бақылануы және жаңартылуы керек. Бұған жаңа қауіптер мен осалдықтарды бақылау және қауіп ландшафтының өзгеруіне қарай қауіпсіздік шараларын жүйелі түрде жаңарту кіреді.

IoT қауіпсіздігі тұрақты негізде жүргізілетін техникалық және процедуралық қауіпсіздік шараларын қамтитын үздіксіз процесс екенін атап өткен жөн. Сонымен қатар, Интернетке қосылған кез келген құрылғы істен тыс шығуға және эксплуатацияға осал. Заттар интернеті дәуірінде біреу жеке деректерге қол жеткізу, зиянды бағдарламаны тарату немесе белгілі бір зиян келтіру үшін пайдалана алатын миллиардтаған қосылған құрылғылар бар. IoT желісінің қауіпсіздігі өндірушілер үшін де, соңғы пайдаланушылар үшін де маңызды болып қала береді, өйткені мемлекеттік органдар, кәсіпорындар мен тұтынушылар IoT қосымшаларының көбеюін пайдаланады және оларға сенеді. Дегенмен, IoT қауіпсіздігі ауыртпалығының бір бөлігі соңғы пайдаланушылардың иығына түседі, өндірушілер де қауіпсіздік шараларын қамтамасыз ету керек. Бұл ортақ жауапкершілік[1].

1.2 Деректерді қорғау және пайдаланушының құпиялылығы үшін IoT қауіпсіздігінің маңыздылығы

Деректерді қорғау – бұл маңызды деректерді зақымданудан, бұзылудан немесе жоғалудан қорғау және деректер қол жетімсіз немесе жарамсыз болып қалса, оны пайдалануға жарамды күйге келтіруді қамтамасыз ету процесі.

Деректерді қорғау оның зақымданбауын, тек рұқсат етілген мақсаттарда пайдаланылуын және қолданыстағы заң немесе нормативтік талаптарға сәйкестігін қамтамасыз етеді. Қорғалған деректер қажет кезде қолжетімді және мақсатқа сай болуы керек.

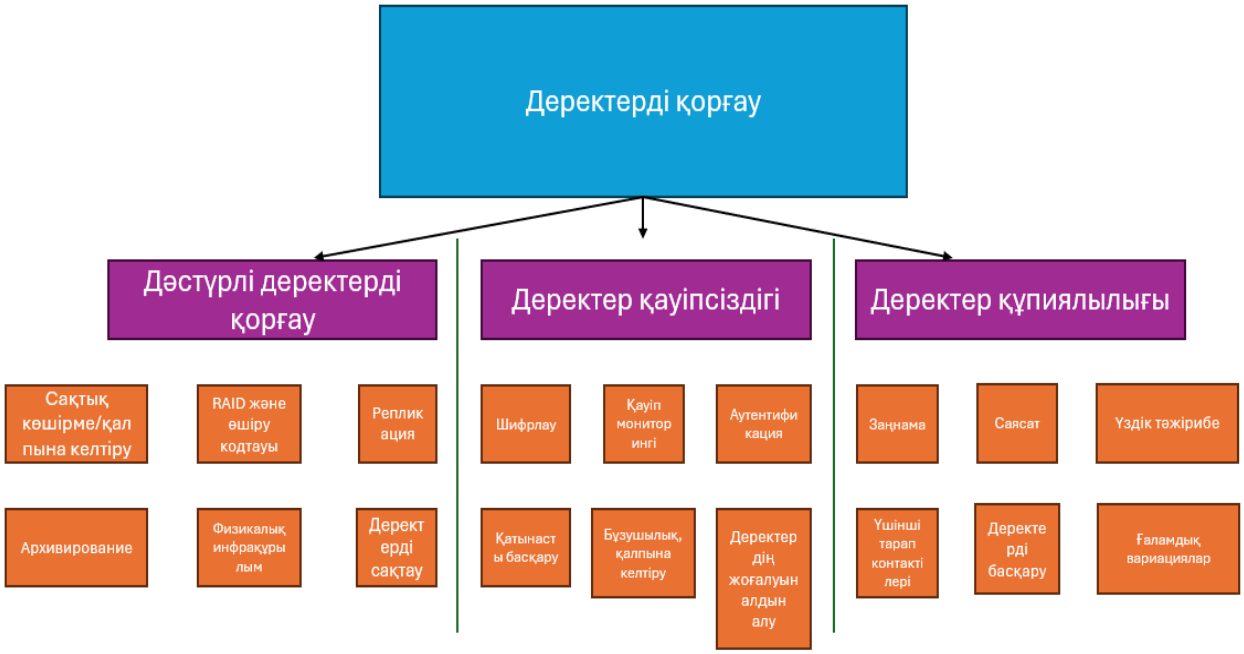
Дегенмен, деректерді қорғау ауқымы қол жетімділік және ыңғайлылық ұғымдарының шеңберінен шығып, өзгермейтіндік, сақтау және деректерді жою/жою сияқты салаларға таралады.

Жалпы, деректерді қорғауды төмендегі диаграммада көрсетілгендей үш кең санатқа бөлуге болады (1.1 сурет): дәстүрлі деректерді қорғау (мысалы, сақтық көшірме жасау және қалпына келтіру), деректер қауіпсіздігі және деректердің құпиялылығы. Деректерді қорғау және қауіпсіздікті қамтамасыз ету үшін пайдаланылатын процестер мен технологияларды маңызды бизнес деректерінің үздіксіз қолжетімділігі мен өзгермейтіндігінің жалпы мақсатына қол жеткізетін деректерді қорғау механизмдері мен іскерлік тәжірибе ретінде қарастыруға болады.

Деректерді қорғау принциптері - деректерді қорғау және оның барлық жағдайларда қолжетімділігін қамтамасыз ету үшін әдістер мен технологияларды пайдалану.

Деректерді сақтау технологияларының көмегімен көшірмелердің сақтық көшірмесін дискіге, таспаға немесе бұлтқа жасау және жоғалған немесе үзілген жағдайда пайдалануға болатын деректер көшірмелерін қауіпсіз сақтау арқылы қорғауға болады. Қосымша бағдарламалық құралдар (мысалы, клондау, көшіру, репликация, суретке түсіру және өзгерту блогын қадағалау) дәстүрлі сақтық көшірмеге қосымша деректерді қорғаудың басқа деңгейін қамтамасыз етеді. Технологиялық жетістіктердің арқасында деректерді үздіксіз қорғау әдеттегі жағдайға айналды, мұнда деректер өзгерген сайын сақтық көшірмелер жасалады, бұл қалпына келтіруді бірден дерлік етеді.

Бұлттық сақтық көшірме де кең таралған, ұйымдар деректердің сақтық көшірмелерін жалпыға қолжетімді бұлттарға немесе үшінші тарап қызмет провайдерлері басқаратын бұлттарға көшіреді. Бұл сақтық көшірмелер жергілікті дискілерді немесе таспа кітапханаларын алмастыра алады немесе апатты қалпына келтіру үшін деректердің қауіпсіз қосымша көшірмесі ретінде әрекет ете алады.



1.1-сурет – Деректерді қорғаудың үш категориясы

Сенсорлық құрылғылар мен қолданбалар арқылы пайдаланушылар мен олардың айналасы туралы құнды және жеке ақпаратты жинай алатын Интернет заттарына қосылған көптеген құрылғылар бар. Кейбір құрылғылар бұл ақпаратты желілер мен Интернет арқылы шифрлаусыз немесе тиісті аутентификациясыз жібереді. Бұл деректерге рұқсат етілмеген адамдар қол жеткізген жағдайда, деректерді дұрыс пайдаланбауға немесе ұрлауға өте осал етеді. Құпиялылық смарт үйлер, смарт желілер, смарт қалалар және қорғаныс жүйелері сияқты IoT жүйелерінде басты мәселе болып табылады. Сондықтан, білім саласы мен зерттеулер немесе белгілі бір мемлекеттің халықтың жеке деректердің құпиялылығын қамтамасыз етілуі керек.

1.3 IoT технологиясындағы қауіпсіздіктің негізгі аспектілері

Жалпы, қауіпсіздік компьютерде пайда болғаннан бері әрқашан басты мәселе болды. Адамдар өздерінің құпиялылығы мен жеке басын сақтай отырып, қауіпсіз жұмыс ортасын қамтамасыз ету үшін технологияға қатты сенеді. Заттар интернетінің пайда болуы есептеу ортасын оқшауланған жүйелерден бейімделгіш және бірлескен жүйелерге айналдырды. Демек, бұл ауысым басып кіру қаупінің артуына байланысты қауіпсіздік мәселелерін тағы да арттырады. Бұл қауіптер жеке ақпараттың ағып кетуінен қаржылық транзакцияны бұзуға және жалған шабуылдарға дейін ауытқиды. Күрделі алгоритмдерді басқаратын смарт құрылғылар зиянды бағдарламаларға әсіресе осал. Сонымен қатар, бұл құрылғылардың ортақ ынтымақтастық платформалары арқылы өзара байланысы қауіпсіздікті бұзу қаупін арттырады.

Қауіпсіздік IoT технологиясының ажырамас тамыры. Оны қолданатын орталар бизнес болсын, өндіріс саласы болсын, әр ұйым өз саласын елге ұсыну барысында өз ақпарат ортасының және де тұтынушының деректерін қалай сенімді түрде сақтау керектігі жайлы нақты іс-жоспарлары болуы тиіс.

Іс-жоспарымыз іске асу үшін негізгі аспектілерді ескеру жөн. Ол аспектілер:

1) Аутентификация және авторизация IoT желілері саласындағы маңызды қолданбалары болып табылады. Олар желіге кіруді қалайтын құрылғылардың да, пайдаланушылардың да жеке басын тексеруге және олардың кіру құқықтарын басқаруға қызмет етеді. Түпнұсқалық растама құрылғының немесе пайдаланушының кім екеніне кепілдік береді, ал авторизация белгілі бір әрекеттерді орындау үшін қажетті рұқсаттарды белгілейді.

2) Ақпараттың құпиялығын қамтамасыз ету үшін деректерді шифрлау маңызды рөл атқарады. Бұл деректерді желі арқылы тасымалдау немесе IoT құрылғыларында сақтау алдында шифрлау үшін криптографиялық алгоритмдерді пайдалануды қамтиды. Осылайша, рұқсат етілмеген адамдар құпия деректерге қол жеткізе алмайды.

3) Деректердің тұтастығы – деректердің тасымалдау және сақтау үдерісінде бастапқы түрінде сақталуын қамтамасыз ететін тағы бір маңызды аспект.

4) Қауіпсіздік шараларын күшейту үшін зиянды бағдарламалар мен бұзудан туындайтын қауіптерді жою қажет. Бұл зиянды бағдарламаларды енгізу немесе жүйеге рұқсатсыз кіру сияқты IoT құрылғыларына жасалған шабуылдарды анықтау және алдын алу шараларын жүзеге асыруды талап етеді. Вирусқа қарсы бағдарламалық құралды, брандмауэрлерді пайдалану және осалдықтарды жою үшін бағдарламалық құралды үнемі жаңартып отыру осы кешенді тәсілдің бір бөлігі болып табылады.

5) Физикалық қауіпсіздік IoT құрылғыларын рұқсат етілмеген физикалық қол жеткізуден және манипуляциядан қорғаудың маңызды факторы болып табылады. Шаралар жоғалған немесе ұрланған жағдайда құрылғыны құлыптау немесе оның деректерін қашықтан өшіру үшін қауіпсіз корпустарды, физикалық құлыптарды және қашықтан басқару механизмдерін пайдалануды қамтуы мүмкін.

6) Желінің қауіпсіздігі Интернет желісінің инфрақұрылымын әртүрлі шабуылдардан, соның ішінде қызмет көрсетуден бас тарту (DDoS) шабуылдары, деректерді тыңдау және маршруттық шабуылдардан қорғау шараларын қамтиды. Желіні қорғау үшін шифрлау, аутентификация және қол жеткізуді басқару қолданылады.

7) Ақырында, қолданбалар мен бұлттық қызметтердің қауіпсіздігі ең маңызды болып табылады. IoT құрылғыларымен байланысу үшін пайдаланылатын бағдарламалық жасақтаманың қауіпсіздігін, сондай-ақ IoT деректерін сақтау және өңдеу үшін пайдаланылатын бұлттық қызметтердің қауіпсіздігін қамтамасыз ету өте маңызды. Тұрақты осалдықты бағалау, бағдарламалық құралды жаңарту және қауіпсіздікті бақылау мен талдау

механизмдерін енгізу осы қауіпсіздік жүйесінің маңызды құрамдас бөліктері болып табылады.

1.3.1 IoT желілеріндегі қауіпсіздік мәселелері

Интернет (IoT) желілері жеке құрылғылардың және бүкіл желінің қауіпсіздігіне теріс әсер ететін көптеген маңызды қауіпсіздік мәселелеріне тап болады. IoT желілеріндегі негізгі қауіпсіздік мәселелеріне: құрылғы қауіпсіздігінің жеткіліксіздігі, қауіпсіздік жаңартуларының болмауы, аутентификация мен авторизацияның әлсіздігі, деректерді шифрлаудың болмауы және желі деңгейіндегі шабуылдарға бейімділік жатады.

IoT қауіпсіздік мәселелері тағы қандай болу мүмкін? IoT құрылғылары мәселенің үлкен бөлігі болып табылады, бірақ жай ғана оларға назар аудару қауіпсіздіктің неліктен маңызды екенін және оның нені қамтитынын толық көрсетпейді. Көптеген нәрселер IoT қауіпсіздігін бүгінгі күні өте маңызды етеді. IoT қауіпсіздігі өте маңызды, өйткені хакерлердің желілерге шабуыл жасау және оларға зиян келтіру жолдары көп. Көптеген адамдар мен компаниялар өздерінің IoT құрылғыларын қалай қорғау керектігін білмеуі мүмкін, бұл оларды шабуылдарға осал етеді. Бұл қауіпсіздік мәселелері әлсіз жақтарды қамтиды. Әлсіздік – пайдаланушылар мен ұйымдарды үнемі мазалайтын үлкен мәселе. IoT құрылғыларының қауіпсіз болмауының себептерінің бірі – олардың өзін қорғауға жеткілікті күші жоқтығында. Барлық жерде осалдықтардың болуының тағы бір себебі – қауіпсіз микробағдарламаны жасау және оны тексеру үшін финанстық жағдайды ескере отырып жеткіліксіз болу мүмкін. Себебі, қолданыстағы құрылғылары арзан әрі тез жасалынғандықтан. Күшті емес, қарапайым құрамдас бөліктер Ripple20 және URGENT/11 сияқты, көптеген құрылғыларға қиындық тудыруы мүмкін. Құрылғылардан басқа, веб-қосымшалардағы және IoT құрылғыларына арналған байланысты бағдарламалық құралдағы әлсіздіктер жүйелерді бұзу қаупіне ұшырауы мүмкін. Зиянды бағдарлама жасайтын адамдар шабуыл жасау мүмкіндіктерін іздейді және олар ескі әлсіз жақтарды пайдалану жолдарын біледі.

Зиянды бағдарлама – компьютер жүйесін зақымдауына арналған бағдарламалық құрал түрі. Көптеген IoT құрылғыларының қуатты есептеу қабілеті болмаса да, олар әлі де зиянды бағдарламаны жұқтыруы мүмкін. Бұл соңғы жылдары интернеттегі жаман адамдар өте жақсы қолданатын нәрсе. IoT зиянды бағдарламасы кең таралған, себебі ол әртүрлі әрекеттерді орындай алады және жаман адамдар үшін көп ақша таба алады.

2016 жылы үлкен шабуыл болды, онда Mirai маңызды веб-сайттар мен қызметтерді жою үшін тұрақты IoT құрылғыларын пайдаланды. Зиянды бағдарламалардың басқа түрлеріне криптовалюталарды ұрлайтын, криптовалютаны өндіруге арналған зиянды бағдарлама және төлем төленгенге дейін компьютер файлдарын құлыптайтын ransomware кіреді.

Интернеттегі шабуылдар санының артуы: Jailbreak құрылғылары DDoS шабуылдарын іске қосу үшін жиі пайдаланылады. Ұрланған құрылғыларды

көбірек машиналарды жұқтыру және жаман әрекетті жасыру немесе компания желісін айналып өту әдісі ретінде пайдалануға болады. Ұйымдар әдетте кибершабуылдардың негізгі нысанасы болғанымен, смарт үйлер көптеген күтпеген киберқылмыстарға тап болады.

Ақпаратты ұрлау және белгісіз тәуекелдерге ұшырау: Интернетке қосылған барлық заттар сияқты қосылған құрылғылардың болуы, желіде болу ықтималдығын арттырады. Құнды ақпаратты ешкім білместен осы құрылғыларда сақтауға және бағыттауға болады. Құрылғыларды пайдалану проблемалары және олардың дұрыс емес конфигурациясы. Қауіпсіздікті елемеу, әлсіз құпия сөздерді пайдалану және құрылғыларды дұрыс басқару бұл қауіптердің сәтті болуына көмектеседі. Кейбір адамдар құрылғыларын қалай қауіпсіз ету керектігін білмеуі мүмкін, сондықтан компаниялар оларға көмектесуі керек. Жаңа проблемалар туындауда, өйткені сала орталығы алдағы болатын мәселені ойламаған. Бұл өсіп келе жатқан IoT жүйелерінде жоспарлар жасауға және жалпы тәуекелдерден қорғауға жеткілікті уақыт болмағанын білдіреді. Жаңа сынақтарға дайындалу – IoT қауіпсіздігін зерттеуді жалғастыруымыздың себептерінің бірі.

2020 жылы Америка Құрама Штаттарының үй шаруашылықтарында көптеген адамдарда Интернетке қосыла алатын орта есеппен 10 құрылғы болды. Бұл зерттеу күрделі IoT орталарын кем дегенде 10 IoT құрылғыларының қосылған желісі ретінде анықтады. Адамдар үшін мұндай ортаны басқару және бақылау өте қиын, өйткені оның өзара байланысты көптеген күрделі бөліктері бар. Бұл жағдайдағы қатені елемеу күрделі проблемаларды тудыруы мүмкін және сіздің үйіңіздің қауіпсіздігін азайтады.

Covid-19 пандемиясы 2020 жылға арналған көптеген жоспарларды өзгертті. Бұл көптеген компанияларды өз қызметкерлеріне үйден жұмыс істеуге мүмкіндік беруге мәжбүр етті және адамдардың үйдегі интернетке көбірек сенуіне себеп болды. IoT құрылғылары көптеген адамдар үшін өз жұмысын үй параметрлерінен орнату үшін пайдалы болды. Бұл өзгерістер бізге IoT құрылғыларын қалай сақтау керектігін тағы бір рет қарау керек екенін көрсетті. 5G – жылдам интернет қосылымы. 5G-ге көшу көптеген адамдарды қызықтырды және үміттендірді. Бұл басқа технологиялардың өсуіне көмектесетін прогресс. Қазіргі уақытта 5G бойынша зерттеулердің көпшілігі оның бизнеске қалай әсер ететініне және оны қалай қауіпсіз пайдалана алатынына бағытталған. Заттар интернетіндегі кибершабуылдардың нәтижесі өте нашар болуы мүмкін. Олар көп зиян келтіруі мүмкін. Заттар интернеті желідегі және нақты әлемдегі жүйелерді түрлендіру мүмкіндігіне ие. IoT жүйелеріне кибершабуылдар күтпеген проблемаларды тудыруы мүмкін, себебі олар нақты әлем проблемаларына оңай әкелуі мүмкін. Бұл, әсіресе, алдыңғы кибершабуылдар ауыр зардаптарды көрсеткен Өнеркәсіптік Интернет заттары (Industrial IoT) аймағына қатысты. Сонымен қоса, денсаулық сақтау саласында пациенттердің маңызды белгілерін алыстан тексеру үшін шағын электронды құрылғылар қолданылады. Бұл құрылғылар пандемия кезінде өте пайдалы болды. Бұл құрылғыларда зиянды әрекеттерді орындау пациенттердің жеке ақпаратын ашуы немесе тіпті олардың

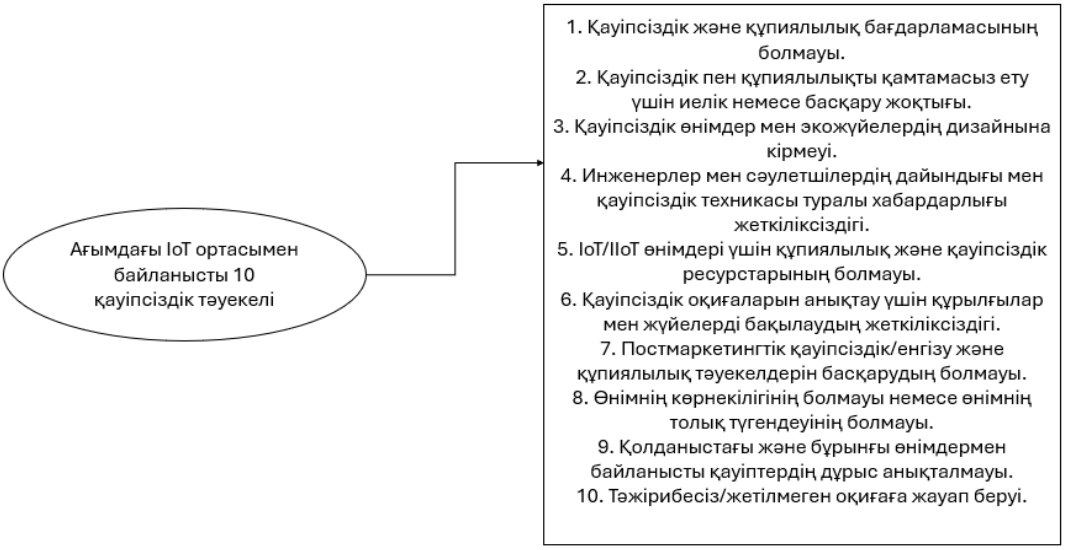
денсаулығы мен қауіпсіздігіне қауіп төндіруі мүмкін. Смарт үйде, құрылғылар қорғалмаған болса, кибершабуылшылар үй шаруашылығына тыңшылық жасап, смарт құлыптар сияқты қауіпсіздік құрылғыларын бұзып, құрылғыларды иелеріне қарсы жұмыс істеуге мәжбүр етуі мүмкін.

1.4 IoT технологиясында үздіксіз байланыстың қауіптері мен тәуекелдері, талаптары және байланысты қорғау әдістері

Заттар интернеті (IoT) желілік қосылымдар санының артуы мен оның ауқымдылығы мен бейімделуіне ықпал ететін жалғанған құрылғылардың алуан түрлілігінің арқасында бүгінгі таңда қол жетімді ең әмбебап технологиялардың бірі ретінде ерекшеленеді.

Заттар интернеті тамақ, өндіріс, қаржы, денсаулық сақтау және энергетика сияқты әртүрлі салаларда, әсіресе заттардың өнеркәсіптік интернеті (IIoT) деп аталатын кеңейту арқылы төңкеріс жасады. Сонымен қатар, заттар интернеті смарт үйлердің, ғимараттардың және тіпті қалалардың дамуына ықпал етті.

Дегенмен, IoT енгізу жүйелер мен құрылғыларға сәтті шабуылдарға әкелуі мүмкін қауіпсіздік тәуекелдерімен бірге келетінін мойындау өте маңызды. Deloitte Risk & Financial Advisory және Dragos кибер-тәжірибесі қауіпсіздік және құпиялылық бағдарламасының жоқтығы, қауіпсіздік пен құпиялылыққа иелік етудің немесе басқарудың жоқтығы сияқты мәселелерді қамтитын қазіргі IoT ортасымен байланысты 10 қауіпсіздік тәуекелін анықтады. Сондай-ақ, инженерлер мен сәулетшілердің қауіпсіздік техникасы бойынша білім деңгейі де жетіспейтіні анықталды.



1.2-сурет – IoT ортасымен байланысты 10 қауіпсіздік тәуекелі

IoT құрылғыларының қауіпсіздігін қамтамасыз ету үшін IoT жүйелерін әзірлеу және қолдау кезінде қауіпсіздікке басымдық беру маңызды. IoT жүйесі

жұмыс істейтін ортаның көлеміне немесе сипатына қарамастан, жүйенің барлық аспектілерін тиімді шешу үшін жобалау кезеңінде қауіпсіздік мәселелерін қарастыру қажет.

IoT қауіпсіздігін жақсарту бойынша ұсынымдар барлық жиналған деректер мен сақталған ақпаратты жан-жақты талдауды және IoT жүйелерінің барлық құрамдас бөліктеріндегі ықтимал осалдықтардан қорғау үшін сенімді қауіпсіздік шараларын енгізуді қамтиды.

Заттар интернеті ұйымға орналастырылған немесе енгізілген жаңа құрылғылардың үлкен санына әкеледі. Әрбір қосылған құрылғы IoT инфрақұрылымына немесе жеке деректерге әлеуетті кіру нүктесі бола алады. Бұл құрылғылардан жиналған деректерді талдауға және тиісті шаралар қолдануға болады. Бұл деректерді талдау жеке тұлғалар немесе ұйымдар үшін құпиялылық мәселелерін тудыруы мүмкін бұрын байқалмаған байланыстарды көрсетеді. Деректер қауіпсіздігі мен құпиялылық мәселелері маңызды, бірақ Интернет заттарымен байланысты ықтимал тәуекелдер жаңа деңгейге көтеріледі, өйткені өзара әрекеттесу, араласу және автономды шешім қабылдау күрделілікті, қауіпсіздік саңылауларын және ықтимал осалдықтарды тарта бастайды. IoT-да, әлбетте құпиялылық тәуекелдері туындайды, өйткені күрделілік қызметке байланысты үлкен осалдықтарды тудыруы мүмкін. IoT-да ақпараттың көп бөлігі адамның туған күні, орналасқан жері, бюджеті және т.б. сияқты жеке ақпараттарға қол жеткізуге мүмкіндік береді. Бұл үлкен деректерден туындайтын қиындықтардың бір аспектісі және қауіпсіздік мамандары осы деректер жиынымен байланысты әлеуетті құпиялылық тәуекелдері туралы ойлануы керек. Заттар интернеті құқықтық мәселелерді, жүйелік тәсілдерді, техникалық мәселелерді және бизнес мәселелерін ескере отырып, құқықтық, этикалық, әлеуметтік және саяси тұрғыдан қолайлы түрде жүзеге асырылуы керек. Сондықтан, Интернет заттарының қауіпсіздік архитектурасын ескеруіміз керек, ол техникалық жағынан біздің деректерімізді қорғау үшін, ісімізді жүзеге асыруына бағытталған, оған орай, IoT қауіпсіздігі бүкіл өмірлік цикл бойы, бастапқы дизайннан бастап қызметтерді іске қосуға дейін қамтамасыз етілуі керек.

Қауіпсіздік – IoT-тегі басты мәселе бола тура, IoT-тегі ең маңызды қауіпсіздік пен деректердің құпиялылығының қандай мәселелері маңызды екені адамзатқа әлі нақты емес. Себебі, кибершабуыл белгілі бір тұлғаға немесе ұйымға әр-түрлі келуі мүмкін. Қауіпсіздік пен деректердің құпиялылығына қатысты мәселелер IoT үшін жаңалық емес; радиожиілік сәйкестендірудің (RFID) алғашқы күндерінен бастап осыған ұқсас мәселелер туындады. Мысалы, RFID белгісі бар электрондық төлқұжат төлқұжатпен жабдықтала бастағанда, деректерді eBay-де 250 долларға қолжетімді жабдықты пайдаланып 30 фут қашықтықтан оқуға болады.

Адамзат RFID тегтеріне өзгертулер енгізуге мәжбүр болды және тегтердің жаңа буыны неғұрлым қауіпсіз болса да, заттар интернетімен байланысты тәуекелдер жаңа деңгейге көтеріледі, өйткені өзара әрекеттесу, коллаждар және

автономды шешім қабылдау күрделі қауіпсіздік саңылауларын және ықтимал қараны тарта бастайды.

1.3-сурет – IoT қауіпсіздігін қорғау талаптары

Кәдімгі желілік жүйелердегі сияқты, сурет 1.3-суретте қарапайым IoT құрылымының қауіпсіздік талаптары көрсетілген, ол негізгі қауіпсіздік талаптарын алты аспектіден қарастырады:

- Құпиялылық (Confidentiality) – деректерді уәкілетті тұлғалар қорғайды;
- Тұтастық (Integrity) – деректерге сенуге болады;
- Қол жетімділік (Availability) – деректер кез келген уақытта және кез келген жерде қолжетімді;
- Бас тартпау (Nonrepudiation) – қызмет аудиттің сенімді ізін қамтамасыз етеді;
- Түпнұсқалық (Authenticity) – құрамдас бөліктер өздерінің сәйкестігін растай алады;
- Бейресми (Privacy) – қызмет тұтынушы деректерін автоматты түрде көрмейді.

IoT өнімдері өз қызметтерімен байланысты деректерді жинап, біріктірген сайын, құпиялылықты қалай сақтау керектігі, қандай әдістер қолдану керектігі жайлы сұрақтар туындай бастайды. Сонымен қатар, уақыт, орын, жиілік және басқа факторлар негізінде деректердің бірнеше биттері жиналып, талданса, алынған деректер тез арада жеке ақпаратқа айналуы мүмкін. Бұл үлкен деректер дилеммасының талданатын ең маңыздыларының бірі; қауіпсіздік сарапшылары деректерді толық жинаумен байланысты кез келген құпиялылық тәуекелдерін ескеретініне көз жеткізуі керек. Интернет заттары контекстінде деректердің құпиялылығы, құпиялылық және сенім қауіпсіздіктің ең үлкен мәселелерін тудырады.

Кәсіпорындар деректерді қорғау протоколдары мен қауіпсіздік жағдайын жақсарту үшін келесі құралдар мен технологияларды пайдалана алады:

1) Жобалау кезеңінде IoT қауіпсіздігін енгізу. Талқыланған IoT қауіпсіздік тәуекелдері мен қиындықтарының көпшілігін жақсы дайындықпен жеңуге болады, әсіресе тұтынушыларға, кәсіпорындарға немесе өнеркәсіпке арналған кез келген IoT (IIoT) құрылғысын әзірлеудің басында ғылыми-зерттеу және әзірлеу үдерісі кезінде. Қауіпсіздікті әдепкі бойынша қосу соңғы операциялық

жүйелерді қамтамасыз етумен және қауіпсіз жабдықты пайдаланумен бірге өте маңызды.

IoT әзірлеушілері киберқауіпсіздіктің осал тұстарын жобалау сатысында ғана емес, дамудың әрбір кезеңінде білуі керек. Мысалы, жүргізуші кілтті металл қорапқа немесе үйінің терезелері мен дәліздерінен алыс орналастырса, көлік кілтін бұзудың алдын алуға болады.

2) PKI (public key infrastructure) және цифрлық сертификаттар. PKI бірнеше желілік құрылғылар арасындағы клиент-сервер қосылымдарын қорғай алады. Асимметриялық екі кілтті криптожүйені пайдалана отырып, PKI сандық сертификаттарды пайдалана отырып, жеке хабарламалар мен өзара әрекеттесулерді шифрлауды және шифрды шешуді жеңілдете алады. Бұл жүйелер пайдаланушылар жеке транзакциялар үшін веб-сайттарға енгізетін мәтіндік ақпаратты қорғауға көмектеседі. PKI қауіпсіздігінсіз электрондық коммерция жұмыс істемейді.

3) Желінің қауіпсіздігі. Желілер шабуылдаушыларға Интернет құрылғыларын қашықтан басқаруға үлкен мүмкіндіктер береді. Желілер сандық және физикалық құрамдастарды қамтитындықтан, жергілікті IoT қауіпсіздігі кіру нүктелерінің екі түрін де қамтуы керек. IoT желісін қорғау порттарды қорғауды, портты қайта жіберуді өшіруді және қажет болмаған кезде порттарды ешқашан ашпауды қамтиды; антивирустық бағдарламалық қамтамасыз етуді, брандмауэрді, енуді анықтау және алдын алу жүйелерін пайдалану; рұқсат етілмеген IP мекенжайларын блоктау; және жүйелердің түзетілгенін және жаңартылғанын қамтамасыз ету.

4) API (application programming interface) қауіпсіздігі. API интерфейстері ең күрделі веб-сайттардың негізі болып табылады. Мысалы, белгілі бір туристік агенттіктерді алып оларға бірнеше авиакомпаниялардан рейс туралы ақпаратты бір жерде жинауға мүмкіндік береді делік. Өкінішке орай, бұл байланыс арналарын хакерлер бұзуы мүмкін, бұл API қауіпсіздігін IoT құрылғыларынан серверлік жүйелерге жіберілген деректердің тұтастығын қорғау және тек рұқсат етілген құрылғылар, әзірлеушілер және қолданбалар API интерфейсімен өзара әрекеттесуін қамтамасыз ету үшін маңызды етеді. 2018 T-Mobile деректерінің бұзылуы API қауіпсіздігінің нашарлығының салдарын көрсетті. Ағып кеткен API арқасында мобильді алпауыт 2 миллионнан астам тұтынушылардың жеке деректерін, соның ішінде шот индекстерін, телефон нөмірлерін және шот нөмірлерін ашты.

Жоғарыда айтылғандай ақпараттар көлеміне байланысты біз былай айта аламыз: «Қанша есе адам IoT құрылғыларын қолданса, сонша есе біздің деректерімізге қауіп төнеді», сондықтан адамзатқа сәл қиындау сынақтан өтуге тура келеді. Оның ең басты сұрағы осы IoT байланысындағы деректерді қалай және қандай тәсілмен қолдану керекпіз?

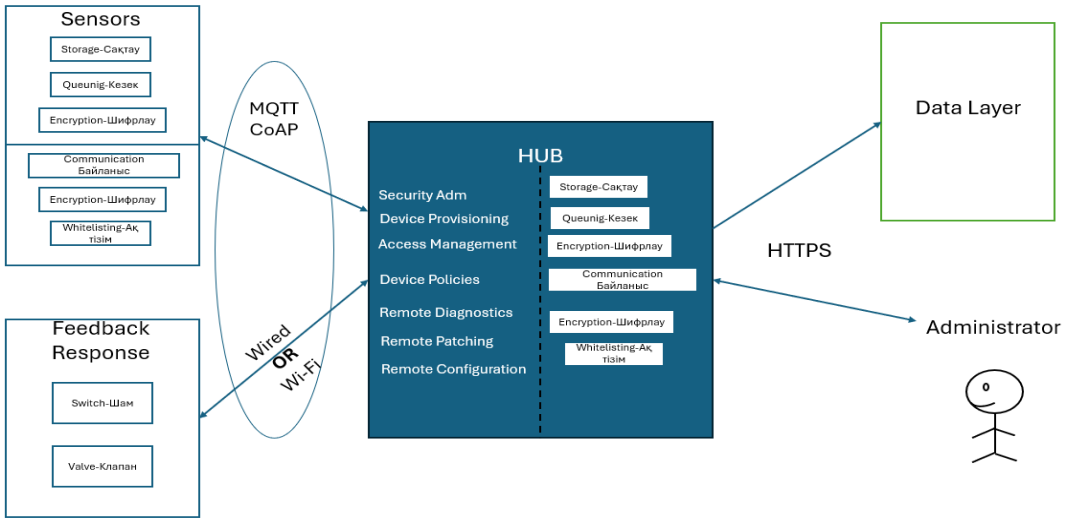
1.4-сурет – IoT байланысын қорғау схемасы

Интернет заттарының қауіпсіздік талаптары жоғары деңгейдегі концептуалды түсінік болып келеді. Ақпарат шеткі деңгейден (яғни, IoT құрылғылары, жинақтар/машиналар) деректер деңгейіне, содан кейін іскери интеллект (BI) деңгейіне, содан кейін 1.4-суретте көрсетілгендей операциялар мен стратегия (OpS) деңгейіне өтеді. Аймақтық желі немесе кең аймақтық желі жергілікті желі құрылғылар мен қабаттарды қосады. Көбінесе көптеген құрылғылар компоненттерді немесе машинаны құрастыруды қолдау үшін біріктіріледі. Құрылғылар арасындағы байланыс жинақта немесе машинада болуы да, болмауы да мүмкін. Құрылғының бірегей функционалдығын инкапсуляциялау және стандарттау мен басқаруды жақсарту үшін құрылғылар мен жинақтар хабқа немесе шлюзге қосылады.

Қауіпсіздікке кешенді көзқарас әр қабаттың қауіпсіздігін және қабаттар арасындағы байланыс қауіпсіздігін қамтиды. Жиектен басқа деңгейлерді жергілікті немесе бұлтта орналастыруға болады.

Ал, енді әр қабатқа немесе деңгейге тоқталсақ. Edge Security (Жиек қауіпсіздігі) – IoT қауіпсіздігіндегі ақпараттық қауіпсіздіктің, байланысының кең тақырыбы болып келеді. Оның ішіндегі ең маңыздысы жиек құрылғылары/датчиктері. Ол, IoT архитектурасының жоғары ағындық құрамдастары арқылы өңделетін деректерді жасайды. Деректердің көлемі Интернетті пайдаланушылардың әрекеттерімен жасалған деректер көлемінен әлдеқайда көп.

Құрылғыға негізделген қауіпсіздік бағдарламалық қамтамасыз ету және IoT хаб/шлюзді басқару бағдарламалық қамтамасыз ету саласында айтарлықтай бәсекелестік бар және көптеген стандарттар қолданады. Microsoft, IBM және Allegro сияқты ұйымдар қолданбалы бағдарламалау интерфейстеріне (API) және жоғары деңгейлі құралдарға құрылғыға негізделген қауіпсіздікті енгізу бойынша белсенді жұмыс жасады. Шеткі қауіпсіздік архитектурасының негізгі құрылысы 1.5-суретте көрсетілген. Хаб немесе шлюз IoT қауіпсіздігіне қатысты қауіпсіздікті басқаруды, сақтауды басқаруды және байланыс құрамдастарын қолдайды.



1.5-сурет – Шеткі қауіпсіздік архитектурасы

Құрылғылар бір-бірімен байланыса алады немесе хабтармен байланыса алады және мұндай байланыс бағдарламалық құралы аз орын мен кезек мүмкіндіктерін қажет етеді. Бұрын, Transmission Control Protocol (TCP) ұяшықтарына негізделген тең дәрежелі байланыстар пайдаланылды, ал қазір одан әрі жетілдірілген хаттамалар пайдаланыста, соның ішінде:

Message Queue Telemetry Transport (MQTT) — құрылғының аутентификациясын, Secure Sockets Layer (SSL)/Transport Layer Security (TLS) шифрлауын, кезекке қоюды және жариялау-жазылу функцияларын қолдайтын TCP негізіндегі протокол.

Шектеулі қолданбалар протоколы (CoAP-Constrained Application Protocol) микроқұрылғыларды қолдайтын және HTTP-ге қарағанда әлдеқайда аз орын алатын пайдаланушы деректерінің протоколы (UDP) негізіндегі тасымалдау болып табылады. Ол Advanced Encryption Standard (AES) шифрлауын қолдайды.

Сымсыз жергілікті желі (WLAN) WPA2 қауіпсіздігі бар көптеген секторларда қолданылады. Қауіпсіздік параметрлері жеткіліксіз болғандықтан және құпия сөзді дұрыс таңдамағандықтан, Wi-Fi қауіпсіздігі жиі бұзылады. Шлюз бірнеше хабтарға қосыла алады және TLS шифрлауын және қарапайым нысанға кіру протоколын (SOAP) өкілдік күйді тасымалдау (REST) хабар алмасуын қолдайтын HTTPS сияқты жоғары деңгейлі байланыс протоколдарын қамтамасыз ете алады.

Құрылғы мен хаб жеткізушілері осы жерде сипатталғандай қауіпсіздік протоколдары мен басқаруды қолдауы керек және бұл қолдау бірнеше протоколдар мен хаттамалар арқылы аутентификацияны қолдауға байланысты күрделі болуы мүмкін.

Бақыланатын тағы бір мәселе. Ол, IoT құрылғыларының істен шығуы. Ақаулық қауіпсіздіктің бұзылуына немесе басқа себептерге байланысты болуы мүмкін. Сәтсіздік құрылғының деректерге қайта кіру әрекетін тудыруы мүмкін және қайталау әрекеттерінің санын шектеу үшін тиісті конфигурациясыз қайталау әрекеттерінің саны шексіз болуы мүмкін. Әрбір қайталау қате туралы

хабарды хабқа кері жібергенде, хаб шексіз қате туралы хабарларды алуы мүмкін (үлестірілген қызмет көрсетуден бас тарту [DDoS] шабуылына ұқсас) және IoT хабы шамадан тыс жүктемеге байланысты істен шығуы мүмкін, бұл хабтың қолжетімділігіне немесе қолданыста болуына кері әсер етеді.

Ақаулық, IoT құрылғысының деректерді жасауына кедергі келтіруі мүмкін. Бұл құрылғылардың арасындағы тұтастығына әсер етеді, сонымен қатар ешбір деректерді қабылдамауына әкеледі. Осылайша, құрылғының ақаулығы IoT қауіпсіздігінің қолжетімділігі мен тұтастығына (ақпараттық қауіпсіздіктің негізгі сапаларына) әсер етуі мүмкін.

Деректер қабаты дәстүрлі дерекқорлар/қоймалар немесе үлкен деректер технологиялары бар Structured Query Language (SQL) немесе NoSQL технологиялары арқылы деректерді қабылдау, деректерді өңдеу және деректерді түрлендіру сияқты әрекеттерді қамтиды. SQL негізіндегі дерекқорлар жол, баған және ұяшық деңгейлерінде қауіпсіздікті қамтамасыз етеді. Үлкен деректер технологиялары бұрын тек файл деңгейінде немесе операциялық жүйе (OS) деңгейінде қауіпсіздікті ұсынатын, бірақ қазір рөлге негізделген авторизациясы бар «Apache Sentry9» сияқты төменгі деңгейлі қауіпсіздікті ұсынады.

Бұл деңгейдегі қауіпсіздік ішкі деңгейлері желілік қауіпсіздікті, аутентификацияны және авторизацияны, масканы немесе стандартты сақтауды шифрлауды, деректерді басқаруды қамтиды. Нашар деректер архитектурасы және/немесе нашар деректер желісін басқару деректердің сәйкестігі мен қолжетімділігін бұзуы мүмкін.

Құпиялылық деректерді сақтауды, қол жеткізуді және беруді реттейтін АҚШ-тың денсаулық сақтандырудың тасымалдануы және жауапкершілігі туралы заңы (HIPAA) және Төлем картасы индустриясының деректер қауіпсіздігі стандарты (PCI DSS) сияқты әртүрлі салалық стандарттарды сақтау арқылы сақталуы керек. ISACA журналының мақаласында; «Құрылғы қауіпсіздігінің болашағына оралу: Құпиялылық пен IoT қауіпсіздік тәуекелдерін белсенді басқару үшін FIPP пайдалану» IoT құрамдастары арқылы жасалған деректерді өңдеу кезінде құпиялылық мәселелерін қалай қарастыру керектігін түсіндіреді.

Деректерді бүркемелеу, рөлге негізделген авторизация және бір рет кіру (SSO-single sign-on) желі қауіпсіздігі мен желіаралық қалқандарға қосымша осы деңгейде қауіпсіздікті қамтамасыз етеді. BI моделін басқару (болжамдық, нұсқамалық) ақпаратты басқару тақырыбы болып табылады. Мұндай модельдер жеткілікті тестілеу мен валидацияны қажет етеді. Қате аналитиканы пайдалану ұйымның беделі мен сенімділігін бұзуы мүмкін ақпаратсыз іскерлік шешімдерге әкелуі мүмкін.

Қосымша қауіпсіздік үшін деректердің жоғалуын болдырмау (DLP-Data Loss Prevention) және сақтық көшірме технологияларыда қолданылады.

Қолданбалардан/жүйелерден құрылғыларға кері байланыс болуы мүмкін. Дәстүрлі желілік қауіпсіздік және желіаралық қалқандар, рөлге негізделген қолданбаға кіру және авторизация және бір реттік кіру осы деңгейде қауіпсіздікті қамтамасыз етеді.

DevOps құралдары жүйенің қолжетімділігіне әсер ететін қате құрастырулар және/немесе қате конфигурациялар қаупін азайтады.

Стратегия BI нәтижелеріне негізделген әрекет бағытын анықтай алады. Стратегия жай ғана IoT құрылғыларынан алынған деректерді бақылау болуы мүмкін немесе ол IoT құрылғыларынан алынған деректерді өңдеуді және құрылғылардан деректерді оқудың рұқсат етілген шектеулеріне негізделген IoT құрылғыларының әрекетін өзгертуді қамтуы мүмкін. Стратегия (талаптар мен дизайн) да, кері байланыс циклі де (іске асыру) сыналауды/тексеруді қажет етеді.

1.4.1 Тақырыптың қойылымы

Бұл қойылым жұмыстың тиімді, қауіпсіз және сенімді жүйелерді құру үшін заттар Интернеті (IoT) желілерінің әртүрлі аспектілерін енгізу және пайдаланудың практикалық тәсілін ұсынады. Әрбір тармақты бөлек қарастыру үшін оларға тақырыптың қысқаша орындалуын беру қажет:

1. Байланыс қауіпсіздігін қамтамасыз ету үшін заттар интернеті протоколдары мен стандарттарын (WPA, WPA2) зерттеу:

WPA және WPA2 протоколдары үйдегі IoT жүйелеріндегі сымсыз желілерді қорғаудың негізгі элементтері болып табылады. Олар смарт үй құрылғылары мен желілік жабдық арасында тасымалданатын деректерді қорғау үшін кеңейтілген шифрлау және аутентификация әдістерін пайдаланады. Бұл хаттамалар желіге рұқсатсыз кіруді болдырмауға көмектеседі және жіберілген ақпараттың құпиялылығына кепілдік береді.

2. Смарт үй желісінің инфрақұрылымын CISCO бағдарламасы арқылы орнату және қауіпсіздікті тексеру:

IoT негізіндегі смарт үйді құрудың бір бөлігі ретінде RADIUS серверімен жұмыс істеу үшін сымсыз маршрутизаторлар мен кіру нүктелерін орнату және конфигурациялау басты назарда. Оны құрау үшін біз CISCO Packet Tracer бағдарламасын қолданамыз. CISCO-дағы RADIUS сервері бүкіл желінің қауіпсіздік деңгейін арттыра отырып, пайдаланушы мен құрылғының аутентификациясын орталықтан басқарады. Қауіпсіздік сынағы әртүрлі шабуыл түрлеріне, соның ішінде бұзу әрекеттеріне және деректерді ұстап алуға қарсы тұру сынауын қамтиды.

3. Қауіпсіз байланысты қамтамасыз ету үшін IoT протоколдарын және WPA немесе WPA2 сияқты стандарттарды пайдалану:

Осы стандарттарды енгізу смарт үй жүйесіндегі деректерді қорғауды қамтамасыз етеді. Сыртқы және ішкі қауіптерден қорғауды барынша арттыру үшін әрбір IoT құрылғысында шифрлау мен аутентификацияны дұрыс орнату басты назарда.

4. Wireshark көмегімен CISCO Packet Tracer бағдарламасының желілік трафигін және байланыс протоколдарын талдау:

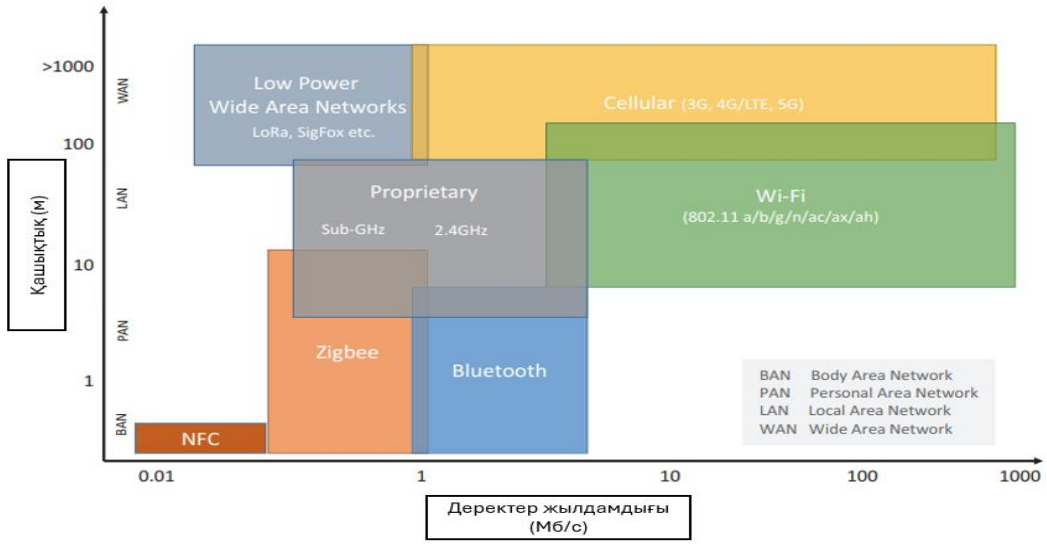
Смарт үй желісіндегі трафикті бақылау және талдау үшін Wireshark пайдалану қауіпсіздік мәселелерін анықтауға және диагностикалауға, сондай-ақ енгізілген қорғаныс шараларының тиімділігін тексеруге мүмкіндік береді. Бұл

құрал желідегі ықтимал қауіптер мен осалдықтарға жылдам жауап беруге мүмкіндік беретін нақты уақытта барлық деректер тасымалдауын бақылауға көмектеседі.

2 IoT технологиялары мен механизмдері

IoT құрылғысын қосу механизмдерін пайдаланған кезде деректер көлеміне бірнеше факторлар әсер етеді, осылайша оны белгілі бір қашықтыққа жеткізуге мүмкіндік береді. Бұл факторларға спектр, арна өткізу қабілеті, таратқыш қуаты, жер бедері, шуға төзімділік және антенна өлшемі жатады. Әдетте, жүру керек қашықтық неғұрлым көп болса, деректер сыйымдылығы соғұрлым аз болады. Ең үлкен таралу қашықтығына жоғары күшейту антеннасы бар төмен жиілікті тар жолақты арнаны пайдалану арқылы қол жеткізуге болады, ал жоғары қуаттарға диапазоны шектеулі кеңірек арналарды таңдау арқылы қол жеткізуге болады. Әрбір қолданба үшін оңтайлы өнімділікке қол жеткізу үшін қажетті өткізу қабілетіне қол жеткізу үшін арна өлшемі, антенна, радиожиілік қуаты және модуляция схемаларының ең жақсы комбинациясын таңдауымыз керек. Радиобайланысты көру желісі ретінде сипаттауға болады, мұнда байланыс құрайтын екі радиостанцияның арасында тікелей оптикалық жол болады. Ол екі радиостанцияның арасында қандай да бір кедергі болған кезде, байланыс көру сызығы пайда болады.

Жақын көрініс (Ближняя видимость) – бұл толық кедергі емес, ішінара кедергі. Жалпы алғанда, төмен жиілікті шешімдер жоғары жиілікті шешімдерге қарағанда жақсы таралу сипаттамаларына ие. Көп ГГц (гигагерц) диапазонында жұмыс істейтін жоғары жиілікті шешімдер әдетте көру сызығы немесе көру сызығына жақын жүйелер болып табылады. 1 ГГц пен 6 ГГц арасында таралу өнімділігі мүмкіндіктері басқа факторларға байланысты өзгереді және әдетте 1 ГГц-тен төмен таралу әлдеқайда жақсырақ болады, бұл жиіліктерді ұзағырақ ауқымдағы қолданбалар үшін қолайлы етеді. 2.1-суретте жалпы сымсыз технологиялар диапазондары мен деректер жылдамдығына арналған барлық мүмкін қосылатын механизмдердің графигі көрсетілген[2].



2.1-сурет – IoT технологиясының қосылыс механизмінің диапозондары және деректер жылдамдықтары

2.1 IoT желілеріндегі деректер алмасу технологиялары

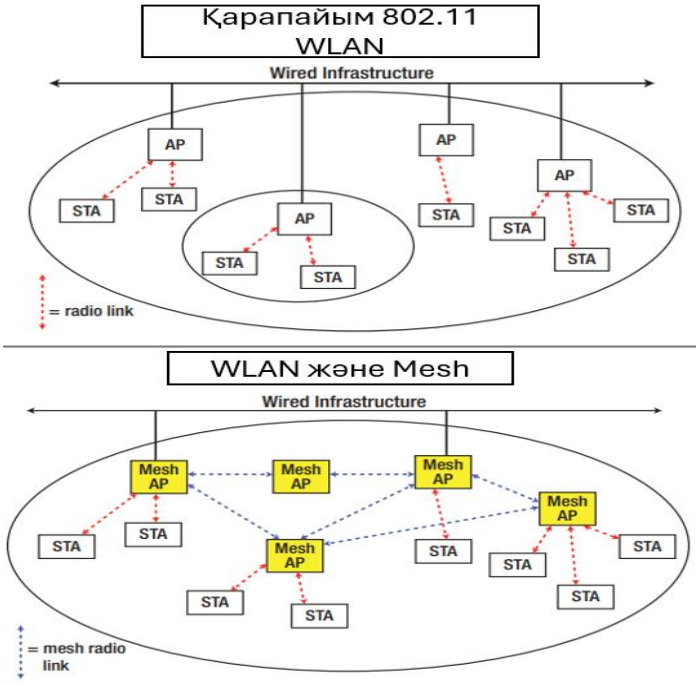
Жұмысты талқылай келе, IoT-тың осы өміріміздегі маңыздылығын ұмытпауымыз керек, себебі бұл заманауи құрылғы бізге Интернетке қосылуға және бір-бірімізбен алыс шақырымдарға деректер алмасуға мүмкіндік беретін физикалық нысанының ажырамас желісі болып саналады. IoT – тің деректер алмасу ортасы біздің күнделіктегі әр сағат, минут, секунд сайын қолданыста болатын бірнеше технологиялар кіреді. Олар: Wi-Fi, Bluetooth, Zigbee, NFC, GPS/GNSS, Cellular, 5G Cellular, LPWAN.

Wi-Fi — IEEE 802.11 стандартына негізделген сымсыз байланыс технологиясы. Алғашында сымсыз жергілікті желі (WLAN) үшін жасалған.

Қолданбаларда Wi-Fi тең дәрежелі және сымсыз жеке аймақтық желі (WPAN) қосылымдары үшін жиі пайдаланылады. Ол қауіпсіз, сенімді және жылдам сымсыз қосылымды қамтамасыз етеді. Wi-Fi желісін электрондық құрылғыларды бір-біріне, Интернетке және Ethernet технологиясын пайдаланып сымды желілерге қосу үшін пайдалануға болады. Ол негізгі сымды желілерге ұқсас нақты жұмыс өнімділігін қамтамасыз ете алады. Wi-Fi желілері 2,4 ГГц және 5 ГГц радио диапазонында жұмыс істейді, кейбір өнімдер екі жолақты да (қос жолақты) қолдайды. Wi-Fi сонымен қатар ультра кең жолақты арналарды және WiGig әзірленген негізгі жолақты шешімді пайдалана отырып, үшінші жолаққа – 60 ГГц диапазонына ауысады. Wi-Fi Alliance — IEEE 802.11 стандартына және олардың өзара әрекеттестігіне негізделген сымсыз технологияларды насихаттайтын сымсыз байланыс саласының ұйымы. Alliance сонымен қатар Wi-Fi үйлесімділігі, қауіпсіздік және қолданбаға арнайы протоколдар бойынша оның техникалық сипаттамаларына сәйкес келетін өнімдерді сертификаттайды. Wi-Fi ұялы байланыспен салыстырғанда төмен қуат

тұтынуды және төмен бағаны қамтамасыз етеді. Wi-Fi-дың ұялы байланыстардан айырмашылығы – лицензияланбаған ауқымда жұмыс істейді, бұл сонымен қатар деректерді тасымалдау құнының төмендеуіне әкеледі. Ауқым сымсыз маршрутизаторға немесе релеге жақындығымен шектелген және желі кептелісіне байланысты қосылым сапасы нашарлауы мүмкін. IoT қолданбалары үшін оңтайландырылған бірнеше түрлі Wi-Fi стандарттарын қолданады. Wi-Fi Direct дәстүрлі Wi-Fi хотспоты болмаған кезде екі немесе одан да көп құрылғыларға тікелей қосылуға мүмкіндік береді. 802.11ac Wi-Fi стандартының кең таралған қолжетімділігімен Wi-Fi кеңірек арналары бар 5 ГГц диапазонында жұмыс істейді (Ескертпе: 802.11n 5 ГГц диапазонында да жұмыс істей алады, бірақ кішірек арналарда), үлкен өткізу қабілетіне мүмкіндік береді. 11ac теориялық өткізу қабілеті 1 Гбит/с-тан асуы мүмкін. 802.11ah, сондай-ақ төмен қуат Wi-Fi ретінде белгілі, 1 ГГц-ден кіші диапазонында жұмыс істейді. Ол кеңейтілген Wi-Fi диапазонын және тиімді қуат тұтыну профилін қолдауды ескере отырып, заттар интернетінің орталық элементі болып саналады. 11ah Wi-Fi жиілік диапазонын 2,4 және 5 ГГц-тен асырып, ғимараттар, жертөлелер және т.б. сияқты қиын орталарда қамтуды қамтамасыз етеді. Ол сондай-ақ қуат күшейткіші жоқ арзан сенсорларды қолдайды және деректердің минималды жылдамдығы қысқа мерзімді деректерге әкеледі. пакеттер. 802.11p - көлік пен көлік байланысының белгіленген стандарты. Ол ақы алу, көліктен көлікке байланыс, қауіпсіздік пен жол бойындағы байланыстар сияқты қолданбалар үшін арнайы қысқа қашықтықтағы байланысты (DSRC) пайдаланады.

IoT қолданбаларына арналған Wi-Fi желілерінің танымалдылығының артуына байланысты кіру нүктесін (AP) сымды желі инфрақұрылымына (мысалы, сымды Ethernet қосқышы) қосу мүмкін емес жерлерде сымсыз желіні қамтамасыз ету қажеттілігі туындады. Әдеттегі мысал, кіру нүктесін үлкен қойманың ортасына қою еді, себебі Ethernet кабелінің ұзындығы 100 метрмен шектелген. Кейбір басқа пайдалану жағдайлары мұнай өңдеу зауыты және т.б. сияқты сыртқы өндірістік аймақтарда Wi-Fi қамтуын қамтамасыз ететін тұрақтағы немесе кампустағы ішкі сымсыз желіні кеңейту болып табылады. Мұндай желі сымсыз қауіпсіздік камералары, қызметтік есептегіштер, ағын мен қысым сенсорлары, көлік құралдарын бақылау жүйелері және т.б. сияқты қолданбаларға қызмет ете алады. 802.11s Wi-Fi тор желісін анықтайды. 2.2 - суретте көрсетілгендей, торлы желілер төменгі жөндеу шығындарымен жылдам орналастыруға мүмкіндік береді және жету қиын аймақтарда қамтуды жеңілдетеді. Негізінде торлы желілер өзін-өзі емдейтін, серпімді және ұзартылатын болып табылады. Қолайлы жағдайларда олар көп реттік бағыттау арқылы желі ауқымын ұлғайтады және көрші түйіндер арасындағы қысқа секірулерден туындаған төмен жіберу қуатының арқасында жоғары өткізу қабілеті мен батареяның қызмет ету мерзімін жақсартады.



2.2-сурет – Классикалық және торлы сымсыз жергілікті желі (mesh wireless local area) топологиялары

Wi-Fi Интернетке қосылу үшін TCP/IP стекін пайдаланады. Wi-Fi технологиясы ноутбуктерде, планшеттерде, смартфондарда және үйдегі ойын-сауық құрылғыларында кең таралғандықтан, тұрмыстық электроника мен кәсіпорын қолданбаларында өте танымал. Wi-Fi қосылу нүктелері қазір стадиондар, әуежайлар, автобустар мен вокзалдар, кафелер мен мектептер сияқты көптеген қоғамдық орындарда орналастырылған. Олар көптеген үйлер мен кеңселерде де бар. Интернетке үнемді және оңай қол жеткізуге сұраныстың артуы, сондай-ақ Wi-Fi Alliance өзара әрекеттесу бағдарламалары мен экожүйелері технологияны бүкіл әлемде кеңінен қолдануды ынталандырды. Оның дүние жүзіндегі қолжетімділігі Wi-Fi-ды арнайы протокол аудармашыларын немесе шлюздерді қажет етпей-ақ, бар инфрақұрылымды пайдалана алатын қолданбалар үшін IoT қосылымының табиғи таңдауына айналдырады.

IoT қолданбаларына арналған Wi-Fi модульдері әдетте РЖ фронтын біріктіреді, осылайша ендірілген жүйе дизайнері үшін кең радио дизайн тәжірибесінің қажеттілігін жояды. Олар АҚШ-тағы FCC (Федералдық коммуникациялар комиссиясы) сияқты нормативтік талаптарға сәйкес болғанымен, көбінесе алдын ала сертификатталған болып келеді, осылайша жүйені сертификаттау процесіне аз уақыт жұмсайды. Wi-Fi бүгінде Интернетке сымсыз қосылудың ең кең таралған технологиясы болып келетіндіктен, олар жоғары қуат тұтынады және күрделілігі IoT әзірлеушілері үшін үлкен кедергі келтіреді, бірақ жаңа кремний құрылғылары мен модульдері осы кедергілердің көпшілігін азайтады және жаңадан пайда болған IoT қолданбалары мен батареямен жұмыс істейтін құрылғыларға Wi-Fi интеграциясын қамтамасыз

етеді. Екінші жағынан, соңғы Wi-Fi стандарттары бейнебақылау, бөлшек сауда және спорт аренасы қолданбаларында қажет болған жағдайда өте жоғары өткізу қабілеттілігі мен сыйымдылықты ұсынады. Осылайша, Wi-Fi көптеген қолданбаларды қолдай алады. 1.1-кестеде қазіргі уақытта 2,4 ГГц және 5 ГГц спектрінде қол жетімді Wi-Fi технологиясының протоколдары жинақталған.

Кесте 1.1 – Wi-Fi протоколдары

Протокол	Жиілігі	Арна ені	MIMO	Максималды деректер жылдамдығы
802.11ac wave2	5 ГГц	80, 80+80, 160 МГц	Multi User (MU-MIMO)	1.73 Гбит/с
802.11ac wave1	5 ГГц	80 МГц	Single User (SU-MIMO)	866.7 Мбит/с
802.11n	2.4/5 ГГц	20, 40 МГц	Single User (SU-MIMO)	450 Мбит/с
802.11g	2.4 ГГц	20 МГц	N/A	54 Мбит/с
802.11a	5 ГГц	20 МГц	N/A	54 Мбит/с
8021.11b	2.4 ГГц	20 МГц	N/A	11 Мбит/с
Legacy 802.11	2.4 ГГц	20 МГц	N/A	2 Мбит/с

802.11ax Wi-Fi желісінің келесі эволюциясын білдіреді. Wi-Fi Alliance Wi-Fi желісінің алтыншы буынын білдіретін IEEE 802.11ax стандартына сілтеме жасай отырып, «Wi-Fi 6» терминін ойлап тапты. Wi-Fi қосылған құрылғылар санының өсуінің жалғасуы, бір пайдаланушыға трафик сұранысының артуы, әр кіру нүктесіне (AP) көбірек пайдаланушылар, жоғары тығыздықтағы Wi-Fi орналастырулары, сыртқы Wi-Fi, гетерогенді құрылғылар мен трафик түрлерінің өсуі, және үлкен қуат пен спектрлік тиімділікке деген ұмтылыс 802.11ax жүйесінің негізгі драйверлері болып табылады. 2,4 ГГц диапазоны Интернет заттары (IoT) қолданбалары үшін Wi-Fi өнімділігін жақсартуға көмектесетін көптеген 802.11ax жақсартуларын ұсынады. Оларға мақсатты ояту уақыты (TWT- target wake time), ортогональды жиілікті бөлу көп қол жеткізу (OFDMA-orthogonal frequency-division multiple access), 2 МГц клиенттері және басқа сымсыз IoT технологияларымен үйлесімділікті жақсарту кіреді. 1 ГГц-тен төмен Wi-Fi HaLow (802.11ah) бүгінгі күнге дейін өте аз қолдау алғандықтан, IoT жүйесінде 2,4 ГГц Wi-Fi үшін әлі де айтарлықтай әлеует бар. Кейбір 2,4 ГГц 802.11ax енгізулері 802.11n немесе басқа қысқа ауқымды IoT сымсыз шешімдерімен салыстырылатын батареяның қызмет ету мерзімін қамтамасыз ете алса, ол бірнеше тік IoT қолданбаларында Wi-Fi үшін жаңа мүмкіндіктер ашуы мүмкін. Стандарт тиімділікті, икемділікті және ауқымдылықты қоса отырып, 802.11ac күшті жақтарына негізделеді. 1.2-кестеде 802.11ac және 802.11ax стандарттары арасындағы негізгі техникалық айырмашылықтар көрсетілген.

Кесте 1.2 – Wi-Fi 802.11ac және Wi-Fi 802.11ax стандарттары арасындағы негізгі техникалық айырмашылықтар

	802.11ac	802.11ax
Жиілігі	5 ГГц	2,4 ГГц/5ГГц
Арна ені	20 МГц, 40 МГц, 80 МГц, 80+80 МГц, 160 МГц	20 МГц, 40 МГц, 80 МГц, 80+80 МГц, 160 МГц
FFT(FastFourierTransform)-жылдам Фурье түрлендіру өлшемі	64, 128, 256, 512	256, 512, 1024, 2048
Ішкі тасымалдаушы аралығы	312,5 kHz	78,125 kHz
OFDM Symbol	3,2 us + 0,8/0,4 us CP	12,8us + 0,8/1,6/3,2 us CP
Ең жоғары модуляция	256-QAM	1024-QAM
Деректер жылдамдығы: 1 кеңістіктік ағын	433 Мбит/с(80 МГц, 1 к.а)	600,4 Мбит/с (80 МГц, 1 к.а)
Деректер жылдамдығы: 8 кеңістіктік ағын (к.а)	6933 Мбит/с (160 МГц, 8 к.а)	9607,8 Мбит/с (160 МГц, 8 к.а)

Wi-Fi қосылу технологиясы үшін қауіпсіздіктің екі аспектісі бар. Біріншісі – желіге және жабдыққа кім қосыла алатынын және конфигурациялай алатынын бақылау. Екінші аспект, Wi-Fi сымсыз желісі арқылы берілетін деректерді шифрлау арқылы рұқсатсыз кіруден қорғау.

Bluetooth лицензияланбаған өндірістік, ғылыми және медициналық (ISM) диапазонында 2,4 ГГц жиілікте таралу спектрін, жиілікті жылжытуды және толық дуплексті сигналды номиналды 1600 сек/сек жылдамдықпен жұмыс істейді. 2,4 ГГц ISM диапазоны көптеген елдерде қол жетімді және лицензияланбаған. Оның диапазоны 1 м-ден 100 м-ге дейін, радионың қай класы қолданылатынына байланысты өзгереді. 2-сынып - ең көп қолданылатын радио. Ол шамамен 10 м диапазонға ие және 2,5 мВт қуат пайдаланады.

Bluetooth тіпті Wi-Fi-мен салыстырғанда аз қуат тұтынумен қысқа қашықтыққа сымсыз қосылымды қамтамасыз етеді. Bluetooth Low Energy (Bluetooth Smart немесе BLE деп те аталады) дәстүрлі Bluetooth қуатын тұтыну профилін одан әрі азайтады. Мысалы, Bluetooth құрылғылары батареяның қызмет ету мерзімін апталар немесе айлар бойы сақтай алады, ал Wi-Fi сағаттар немесе күндер болуы мүмкін. Деректерді беру жылдамдығы шамамен 1 Мбит/с шектелген (бірақ теориялық өткізу қабілеті 24 Мбит/с дейін), бірақ диапазон шамамен 100 метрге (300+ фут) дейін созылады. Wi-Fi сияқты, Bluetooth құрылғыны машинаға қосу және құрылғыны жұптау үшін пайдалануға болады. Bluetooth 4.1 2013 жылдың желтоқсанында ұсынылды, ол деректерді хостқа қайтармас бұрын құрылғыларға бір-бірімен байланысуға мүмкіндік береді және LTE-мен өзара әрекеттеседі. Bluetooth SIG Bluetooth стандартын басқарады. Bluetooth технологиясы бастапқыда телефондар мен компьютерлер арасындағы байланыс стандарты ретінде ұсынылды. Бастапқыда Bluetooth-ды танымал еткен

негізгі пайдалану жағдайы автомобильдердегі гарнитуралармен және көліктегі ақпараттық ойын-сауық жүйелерімен қолсыз телефон қоңыраулары болды. Смартфондардың пайда болуымен жоғары сапалы музыка ағыны мен денсаулық пен фитнес аксессуарлары да танымал бола бастады. Bluetooth – бұл PAN (жеке желі) технологиясы, ең алдымен, қысқа қашықтықтағы байланыс үшін кабельді ауыстыру ретінде пайдаланылады. Оны нүктеден нүктеге немесе жұлдызша желі топологиясында қолдануға болады. Ол сегізге дейін қосылған құрылғылармен 2 Мбит/с дейінгі деректерді өткізу жылдамдығын қолдайды. Түпнұсқа Bluetooth стандарты бүгінде оны Bluetooth Low Energy стандартынан ажырату үшін әдетте Bluetooth Classic деп аталады. Bluetooth төмен энергиясы, кейде Bluetooth Smart деп аталады, Bluetooth сипаттамасына қосымша болып табылады. Bluetooth SIG оны 2010 жылы Bluetooth 4.0 стандартында аз қуатты IoT кеңістігіне кіру үшін қабылдады.

Bluetooth Low Energy 2,4 ГГц ISM жолағын да пайдаланғанымен, ол Bluetooth Classic нұсқасымен үйлесімді емес. Bluetooth Low Energy 40 2 МГц арнаны пайдаланады, ал Bluetooth Classic кеңдігі 1 МГц 79 арнаны пайдаланады. Bluetooth Classic-пен салыстырғанда, Bluetooth Low Energy Bluetooth құрылғыларының қуатты тұтынуын айтарлықтай төмендетеді және төмен деректер өткізу қабілетін қолдайды және батареямен жұмыс істейтін құрылғылардың ұзақ қызмет ету мерзімін қамтамасыз етеді. Bluetooth Low Energy сонымен қатар сигнал беру мүмкіндігі мен орынға негізделген қызметтерді ұсынады. Bluetooth Low Energy өте танымал болып шықты, бұл фитнес, ойыншықтар және автомобиль қолданбалары сияқты әртүрлі кеңістіктерде жаңа қолданбалардың пайда болуына себеп болды. Ол қазір көптеген жаңа Bluetooth стандарттарының негізгі қозғаушы күші болып табылады.

Осы жылдар ішінде Bluetooth SIG негізгі өзгерістерді жариялады

қауіпсіздікті, батареяның қызмет ету мерзімін және IP негізіндегі желілермен оңай әрекеттесуді жақсарту үшін техникалық сипаттамалар. Мысалы, Bluetooth 4.2 спецификациясы эллиптикалық қисық криптографияға (ECC) негізделген кілттерді басқару және хабарды шифрлау үшін шифрлық блок тізбегі хабарламаның аутентификация коды (CCM) криптографиясы бар Advanced Encryption Standard (AES) есептегішімен өнеркәсіптік беріктік қауіпсіздігін қосты.

Bluetooth 5 деректер жылдамдығы мен жұмыс ауқымдары: 2 Мбит/с, 1 Мбит/с, 500 Кбит/с және 125 Кбит/с осы жылдамдықта жұмыс істейді. Деректер жылдамдығы неғұрлым төмен болса, диапазон соғұрлым ұзағырақ болады. Ауқымның және деректер жылдамдығының ұлғаюы Bluetooth Low Energy өнеркәсіптік деректер тіркеушілері немесе смарт қуат есептегіштері сияқты тұтынушылық емес сегменттерде тартымды етеді. Сонымен қатар, Bluetooth Low Energy-дің мобильді құрылғылармен кіріктірілген үйлесімділік артықшылығы, ол деректерді көрсету және іздеу, Интернетке қосылу және өрістегі IoT құрылғыларын бастапқы қамтамасыз ету және конфигурациялау үшін тамаша

таңдау болып табылады. 1.3-кестеде Bluetooth Classic және Bluetooth Low Energy технологияларының салыстырылуы көрсетілген.

2017 жылы Bluetooth SIG тор профилі мен тор үлгісінің сипаттамаларын шығарды. Mesh желілік технологиясы смарт жарықтандыру, төмен қуатты сымсыз сенсорлық желілер және т.б. . Ол, сондай-ақ деректерді желі арқылы жіберу үшін аралық түйіндерді пайдалана отырып, кеңейтілген диапазондағы байланысты қамтамасыз етеді. Бұл жаңа тор стандарттары Bluetooth 5 және Bluetooth 4.x стандарттарымен үйлесімді.

Кесте 1.3 – Bluetooth Classic және Bluetooth Low Energy технологияларының салыстырылуы

	Bluetooth Low Energy	Bluetooth Classic
Модуляциясы	GFSK	GFSK, π/4 DQPSK, 8DPSK
Қуаты	~0,01x ~ 0,5x reference value	1 (reference value)
Деректер жылдамдығы	LE 2M PHY: 2 Мбит/с LE 1M PHY: 1 Мбит/с LE Coded PHY (S=2): 500 Кбит/с LE Coded PHY (S=8): 125 Кбит/с	EDR PHY (8DPSK): 3 Мбит/с EDR PHY (π/4 DQPSK): 2 Мбит/с BR PHY (GFSK): 1 Мбит/с
Шығыс қуаты (Tx)	Class 1: 100 мВт (+20 dBm) Class 1.5: 10 мВт (+10 dBm) Class 2: 2.5 мВт (+4 dBm) Class 3: 1 мВТ (0 dBm)	Class 1: 100 мВт (+20 dBm) Class 2: 2.5 мВт (+4 dBm) Class 3: 1 мВт (0 dBm)
Оңтайландырылған	Қысқа мерзімді деректерді беруге	Үздіксіз деректер ағынына
Қолданылатын жиілігі	2.4 ГГц ISM диапазоны (2,402–2,480 ГГц негізгі диапазоны)	2.4 ГГц ISM диапазоны (2,402–2,480 ГГц негізгі диапазоны)
Арна спектрі	Секіріп таралынатын жиілік спектрі (FHSS- Frequency-Hopping Spread Spectrum (FHSS))	Секіріп таралынатын жиілік спектрі (FHSS- Frequency-Hopping Spread Spectrum (FHSS))
Арналар саны	2 МГц аралығы бар 40 арна (3 жарнамалық арна/37 деректер арнасы)	1 МГц аралықпен 79 арна
Желі топологиясы	Point-to-point (including piconet) BroadcastMesh	Point-to-point (including piconet) BroadcastMesh

Bluetooth тор желісіндегі қауіпсіздік жеке құрылғылардың немесе теңдес құрылғылар арасындағы қосылымдардың қауіпсіздігі туралы ғана емес; ол барлық құрылғылар желісінің және желідегі құрылғылардың әртүрлі топтарының қауіпсіздігіне қатысты.

Сондықтан Bluetooth тор желісінің қауіпсіздігі міндетті болып табылады. Бұған келесі негізгі қауіпсіздік шараларын енгізу арқылы қол жеткізіледі:

- Шифрлау және аутентификация: барлық Bluetooth Mesh хабарлары шифрланған және аутентификацияланған.

- Тапсырмаларды бөлу: Желі қауіпсіздігі, қолданба қауіпсіздігі және құрылғы қауіпсіздігі дербес шешіледі.

- Аймақтарды оқшаулау: Bluetooth тор желісін ішкі желілерге бөлуге болады, олардың әрқайсысы басқалардан криптографиялық тұрғыдан ерекшеленеді және қауіпсіз.

- Кілтті жаңарту: қауіпсіздік кілттерін Bluetooth тор желісінің қызмет ету мерзімі ішінде Кілтті жаңарту процедурасы арқылы өзгертуге болады.

- Хабарды жасыру: хабарды жасыру желі ішінде жіберілген хабарларды қадағалауды қиындатады және осылайша түйіндерді бақылауды қиындататын құпиялылық механизмін қамтамасыз етеді.

- Қайта ойнату шабуылдарынан қорғау: Bluetooth тор желісінің қауіпсіздігі желіні қайта ойнату шабуылдарынан қорғайды.

- Құрылғыларды қауіпсіз қамтамасыз ету: Құрылғыларды Bluetooth тор желісіне қосу және оларды түйіндерге айналдыру процесі қауіпсіз процесс болып табылады.

Zigbee IEEE 802.15.4 сілтеме деңгейіне негізделген және әдетте 2,4 ГГц ISM диапазонында жұмыс істейді. Оның желілік деңгейі ең басынан торлы топология операцияларын ескере отырып жасалған. Бұл желіге көп ретті операциялар арқылы географиялық масштабтауға мүмкіндік береді (смарт есептегіштер сияқты қолданбалар үшін), сондай-ақ ақауларға төзімділік пен сенімділікті жақсартады, өйткені кез келген екі нүкте арасында тор желісі арқылы артық жолдар жасалады.

Zigbee-ді Zigbee Alliance әзірлейді, алға жылжытады және қолдайды. Zigbee 3.0, ең соңғы спецификация, пайдаланушылар мен әзірлеушілер үшін таңдау мен икемділікті кеңейтеді және өнімдер мен қызметтер стектің барлық деңгейлерінде стандарттау арқылы бірге жұмыс істейтініне сенімділік береді. Zigbee 3.0 толық функционалды, сертификатталған және үйлесімді төмен қуатты Zigbee шешіміне тор және қауіпсіздік қабаттары мен қолданбалы жүйені қосу арқылы IEEE 802.15.4 стандартын кеңейтетін Zigbee PRO үстіне құрастырылған. Zigbee нақты құрылғылар арасындағы өзара әрекеттесуге мүмкіндік беретін кешенді шешімді ұсынады. Zigbee протоколдар жинағы Zigbee кластерлік кітапханасын қамтиды: әртүрлі тік нарықтарда жұмыс істейтін және көптеген жылдар бойы сыналған бастапқы жабдық өндірушілері (OEM) жасаған құрылғы түрлерінің, деректер үлгілерінің және мінез-құлықтарының стандартты кітапханасы. Zigbee Alliance басқаратын қатаң сертификаттау бағдарламасы соңғы өнім тұрғысынан құрылғы түрінің әрекеті мен функционалдығын тексеру және әртүрлі өндірушілердің өнімдерінің бірге жұмыс істей алатынын қамтамасыз ету арқылы Zigbee құрылғыларының өзара әрекеттесуін қамтамасыз етеді. Zigbee протокол жиынтығын іске қосу, қауіпсіздік, желі және құрылғыны басқарудың стандартты процедураларын қамтиды. Құрылғылардың әр түрлі түрлері желіге қосылып, аутентификациялауы мүмкін және оларды зауыттық параметрлерге қалпына келтіруге немесе үйлесімді түрде пайдаланудан

шығаруға болады, бұл құрылғының басталуынан бастап құрылғының өзара әрекеттесуін және деректер жинағыштармен немесе хабтармен үздіксіз интеграциялануын қамтамасыз етеді. Zigbee негізіндегі қолданбалар негізінен жарықтандыруға, үйді басқаруға және физикалық қауіпсіздік сегменттеріне назар аудара отырып, ақылды үй мен смарт ғимараттарға бағытталған. Көптеген телекоммуникация, қауіпсіздік және интернет провайдерлері тұтынушыларға үйді автоматтандыру қызметтерін ұсыну кезінде таңдау протоколы ретінде Zigbee-ді және көптеген жарықтандыру өндірушілерінде хаттаманы қолдайтын смарт шамдарды мақұлдады.

Zigbee IEEE 802.15.4 физикалық радиостандартты толық пайдаланады және бүкіл әлем бойынша 2,4 ГГц (жаһандық), 915 МГц (Америка) және 868 МГц (Еуропа) лицензияланбаған жолақтарда жұмыс істейді. 250 Кбит/с шикі деректер өткізу қабілетіне 2,4 ГГц (16 арна), 915-921 МГц (27 арна) кезінде 10 Кбит/с және 868 МГц (63 арна) кезінде 100 Кбит/с жетуге болады. Берілу диапазоны шығыс қуаты мен қоршаған ортаның сипаттамаларына байланысты 10-нан 100 метрге дейін өзгереді. Sub-1 ГГц арнасы бойынша тарату диапазоны 1 км-ге дейін. 1.4-кестеде Zigbee технологиясының қысқаша шолуы берілген. Zigbee құрылғы жұмысына арналған қолданба деректерін де, торды басқару және маршруттау сияқты желіні басқару процедураларын да өте аз қуат тұтынумен жіберу үшін арнайы өткізу қабілеттілігін тиімді пайдаланады. Zigbee адрестеу схемасы желідегі жүздеген түйіндерді (64 КБ дейін) қолдауға қабілетті және өте үлкен желілерді қолдау үшін бірнеше желі координаторларын біріктіруге болады. Zigbee желісінің логикалық өлшемі сайып келгенде, қандай жиілік диапазонының таңдалғанына, желідегі әрбір құрылғы қаншалықты жиі байланысуы керек екеніне және қолданба деректердің жоғалуына немесе қайта жіберілуіне қаншалықты шыдайтынына байланысты.

Кесте 1.4 – Zigbee технологиясының сипаттамасы

Параметрі	Сипаттамасы
Желі протоколы	Zigbee PRO 2015
Желі топологиясы	Self-Forming, Self-Healing MESH
Желілік құрылғысы	Координатор (бағытталатын), маршрутизатор, соңғы құрылғы, Zigbee Green Power құрылғысы
Желі өлшемі (түйіндер саны)	65000-ға дейін
Стандарты	IEEE 802.15.4-2011
Жиілігі/арнасы	2.4 ГГц(ISM диапазоны)/16 арналы ені 2МГц
Деректер жылдамдығы	250 Кбит/с
Қауіпсіздік моделі	Орталықтандырылған (орнату кодтары қолдауымен)
Шифрлау	AES-128 желі деңгейінде, AES-128 қолданба деңгейінде қолжетімді
Байланыс диапазоны	300+ метрге дейін (көру желісі), үй ішінде 75–100 метрге дейін

1.4 кестенің жалғасы

Төмен қуатты қолдануы	ұйқы режимінде, Zigbee жасыл қуат құрылғылары (энергия егін жинау)

Near Field Communication (NFC) — жоғары жиілікті (HF) (13,56 МГц) контактісіз және RFID технологиясынан жасалған қысқа ауқымды сымсыз байланыс технологиясы. ISM диапазонында 13,56 МГц жиілікті және 4 см-ге дейінгі әдеттегі жұмыс қашықтығын пайдалана отырып, NFC бүгінде 106 Кбит/с-тан 848 Кбит/с-қа дейінгі тасымалдау жылдамдығын қамтамасыз етеді. NFC үш түрлі режимде жұмыс істей алатын қысқа ауқымды сымсыз қосылымды жасайды: картаны эмуляциялау, оқу/жазу және тең дәрежелі. NFC технологиясы смартфонның электрондық әмиянына және медициналық қолданбаларға арналған смарт тегтерге кілтсіз кіруден бастап пайдалану жағдайларының кең ауқымын қамтамасыз етеді. Бұл іске асырудың қарапайымдылығымен және тегтерді несие карталарына, смартфондарға және басқа киілетін құрылғыларға ендіру мүмкіндігіне байланысты.

GPS – пайдаланушыларға орналасқан жер, жылдамдық және уақыт туралы ақпаратты беретін спутниктік радионавигация жүйесі. GPS қабылдағышы әрбір көрінетін жерсеріктен сигнал алады және жеке уақыт кешігулерін өлшейді. Осы уақыт кідірістерін белгілі радиотолқынның таралу сипаттамаларына қолдану әрбір жерсерікке дейінгі қашықтықты есептеуге мүмкіндік береді. GPS дәлдігі GPS қабылдағышы сәтті анықтаған жерсеріктердің санына сәйкес келеді. Glonass, Galileo және Compass сияқты жаңа жүйелер әзірленуде, олар GPS-пен бірге пайдаланылғанда жаһандық қамтуды жақсартады, орналасу уақытын қысқартады және қиын орталарда өнімділікті жақсартады. Борттық GPS трекерлері жинаған орын деректері флотты басқару, активтерді қадағалау және автономды көліктер сияқты көлік саласындағы көптеген қолданбалар үшін өте маңызды.

Ұялы технологиялар магистральдық желіге – бұлтқа тұрақты қосылуды қамтамасыз етеді. Тұтынушы қолданбаларына арналған ұялы телефондар сияқты, Интернет заттарының ұялы деректерін 2G, 3G немесе 4G арқылы тасымалдауға болады.

желілер. Артықшылықтары базалық станцияның қолданыстағы инфрақұрылымын пайдалана отырып, кең қамтуды, сондай-ақ ұтқырлықты (мысалы, автомобильдерді) қамтиды. Ықтимал кемшіліктерге қуат тұтыну, байланыс операторларына тиесілі лицензияланған спектр бойынша деректерді жіберуге байланысты төлемдер және қамтудағы ықтимал бос орындар жатады. IoT құрылғыларының барлық жерде қосылуына сұраныс күшейген сайын, ұялы желілер бар желілік инфрақұрылымды пайдалана отырып, сенімді және қауіпсіз IoT қызметтерін ұсына алады. Көптеген елдерде бүкіл халықты жақсы қамтуды қамтамасыз ету үшін спектрді бөлуге және желіні орналастыруға ауқымды инвестициялар салынды. Адамдарды біріктіру үшін пайдаланылатын желілерді енді заттарды қосу үшін пайдалануға болады.

2G, 3G немесе одан жоғары санаттағы 4G модемдері сияқты дәстүрлі ұялы байланыс опциялары көп қуатты тұтынады және смарт есептегіштер, активтерді бақылау құралдары, денсаулық сақтау жабдықтары, ауыл шаруашылығы сияқты деректердің аз ғана көлемі сирек тасымалданатын қолданбаларға жақсы сәйкес келмейді. сенсорлар, тұрақ орындары және көше шамдары. Ұялы IoT қуаты аз, ұзаққа созылатын қолданбалардың талаптарын қанағаттандыру үшін жасалған. Бұл смартфондар үшін біз күнделікті қолданатын қолданыстағы технологияны алады және қуатты аз құрылғылардың қажеттіліктерін қанағаттандыру үшін оны кеңейтеді. Коммуникациялық шешімнің құнын талдауға келгенде, иеленудің жалпы құны спектрлік шығындарды, инфрақұрылымдық шығындарды және операциялық шығындарды қамтиды. Ұялы желілер қазірдің өзінде орнатылғандықтан, өте аз жаңа инфрақұрылымды орнату қажет. Базалық станциялар, ұялы мұнаралар, ғимараттар және электрмен жабдықтау бүкіл әлемде қазірдің өзінде орнатылған. Технология сонымен қатар бір шаршы километрге жүздеген мың IoT құрылғыларын қамту мүмкіндігіне ие, бұл басқа байланыс опцияларына қарағанда әлдеқайда көп. Бірде-бір технология немесе шешім әртүрлі ықтимал жаппай IoT қолданбаларына, нарықтық жағдайларға және спектрдің қолжетімділігіне өте қолайлы. Нәтижесінде мобильді индустрия бірнеше технологияларды стандарттауда, соның ішінде Long-Term Evolution for Machines (LTE-M) және тар жолақты IoT (NB-IoT). NB-IoT өткізу қабілеті төмен, салыстырмалы түрде стационарлық құрылғыдан сирек байланыс үшін өте қолайлы, ал LTE-M жоғары өткізу қабілеттілігіне немесе мобильді және роуминг қолданбаларына сәйкес келеді. NB-IoT үшін жақсы қолданба температураны, желді, қысымды және т.б. өлшеу үшін қашықтағы қоршаған орта сенсорларын пайдалану болып табылады. Бұл құрылғылар батареяны пайдалануды оңтайландыру кезінде тұрақты жаңартуларды тұрақты жерден жібере алады. Мұндай құрылғы 10 жылға дейін немесе күн сәулесінен қуат алатын болса және дұрыс географиялық жағдайда болса, одан да ұзақ қызмет ете алады. Сол сияқты, мобильді және елден елге роумингте жүретін бірнеше сенсорлар арқылы жағдайды бақылайтын актив трекеріне магистральдық жылдамдықты ұтқырлықты, елдер мен операторлар арасындағы халықаралық роумингті және микробағдарламаны тиімді жаңартуды ұсынатын LTE-M шешімі жақсы қызмет көрсетеді.

Заттар интернеті үшін ұялы байланыстың артықшылықтары мыналарды қамтиды:

- Қолданыстағы инфрақұрылымға негізделген ашық стандарттарды қолдану адамдардың тұратын жерінің барлығында дерлік қамтуға қол жеткізуге мүмкіндік береді.

- LTE стандартындағы және лицензияланған спектрдегі жетілдірілген қатар өмір сүру механизмдерінің арқасында көптеген құрылғылар бір уақытта жұмыс істей алады, бұл бүгінде шағын аумақта бір уақытта қолданылатын ұялы телефондардың көптігімен дәлелденді.

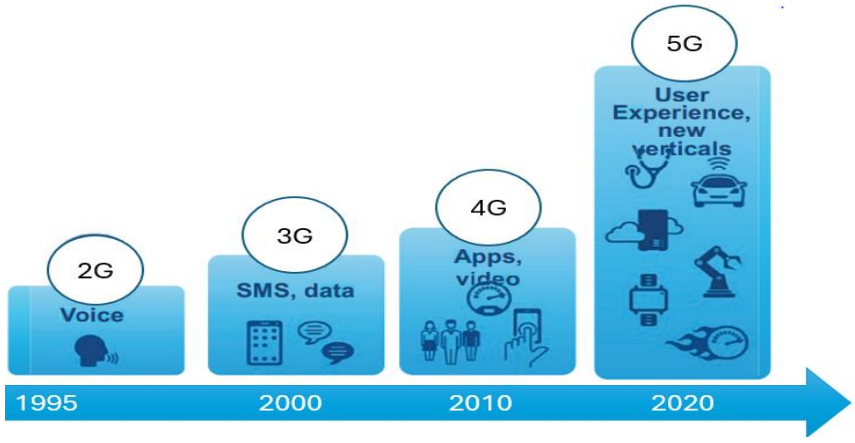
- Ешқандай шектеуші ережелер жоқ, сондықтан сіз 23 дБм дейін тарата аласыз және қажетінше көп эфир уақытын ала аласыз.

- SIM картасының тіркелгі деректерін пайдалана отырып, LTE желісі арқылы шифрлаудың үстіңгі жағындағы қауіпсіздік үшін стандартты TLS/DTLS қауіпсіздігіне қолдау көрсетіледі. Бұл құрылғыдан бұлттық серверге тасымалданатын деректердің қауіпсіздігін қамтамасыз етеді.

- Ұялы желіні қамту көлемі ұлғайған сайын және технологиялар күрделілігі төмен және төмен қуат опцияларында қолжетімді болғандықтан, ұялы байланыс технологиялары дүниежүзілік заттар интернеті қажеттіліктері үшін тамаша таңдауға айналуда.

Бірінші буын (1G) мобильді желі толығымен дауысқа негізделген және аналогтық технологияны пайдаланды. 2G цифрлық технологияны пайдалана отырып, дауыстық және мәтіндік хабар алмасуды (Short Message Service - SMS) қолдайды. 3G дауыс, мәтіндік хабар алмасу және деректер туралы болды. 4G барлығы 3G болды, бірақ жылдамырақ, ал 5G одан да жылдамырақ болады. 5G секундтарда толық метражды HD фильмді жүктеп алу үшін жеткілікті жылдам болады. 2G-ден 4G-ге көшу 2.3-суретте көрсетілгендей шамамен 20 жылда болды.

Ұялы желінің нақты өнімділігі провайдерге, оның желі конфигурациясына, берілген ұяшықтағы белсенді қосылымдар санына, белгілі бір орындағы радио ортасына, пайдаланылатын құрылғының мүмкіндіктеріне және радио өнімділігіне әсер ететін барлық басқа факторларға байланысты болады.



2.3-сурет – Ұялы байланыс технологиясының эволюциясы

Өткізу қабілеттілігі деректерді өткізу мүмкіндігінің төменгі шегіне әлдеқайда жақын болады және кідіріс берілген ұрпақ үшін пакеттік кідірістің жоғары шегіне бейім болады деп болжауға болады. 1.5-кесте ұялы технологиялардың әртүрлі буындарының деректер жылдамдығы мен кідірістерінің қысқаша мазмұнын береді.

5G – бұл өте маңызды және басқа желілерден гөрі әлдеқайда жылдам желі болып саналады. Ол жоғары жылдамдықты қосылымның, өте төмен кідірістің және барлық жерде қамтудың бірегей комбинациясын қолдайды, бұл оны IoT-пен пайдалану жағдайларын қолдау үшін өте қолайлы етеді. 5G бізге нақты

уақыттағы желі өнімділігіндегі маңызды болып табылатын қолданбаларда, көбірек құрылғыларды қашықтан басқаруға мүмкіндік береді.

Кесте 1.5 – Ұялы технологиялардың әртүрлі буындарының деректерді беру жылдамдығы мен кідірістерін салыстыру

Буын	Максималды деректер жылдамдығы	Практикалық деректер жылдамдығы	Кідіріс	Сипаттама
1G	-	-	-	Аналогтық жүйе
2G	100 Кбит/с	100-400 Кбит/с	300-1000мс	қабаттасу немесе аналогтық жүйелерге параллель сияқты алғашқы цифрлық жүйелер
3G	10 Мбит/с	400 Кбит/с-5 Мбит/с	100-500мс	Аналогтық жүйелерге параллель орналастырылған арнайы сандық желілер
4G	100 Мбит/с	1-50 Мбит/с	<100мс	Сандық және тек пакеттік желілер
5G	10 Гбит/с	TBD	1-20мс	Сандық және тек пакеттік желілер

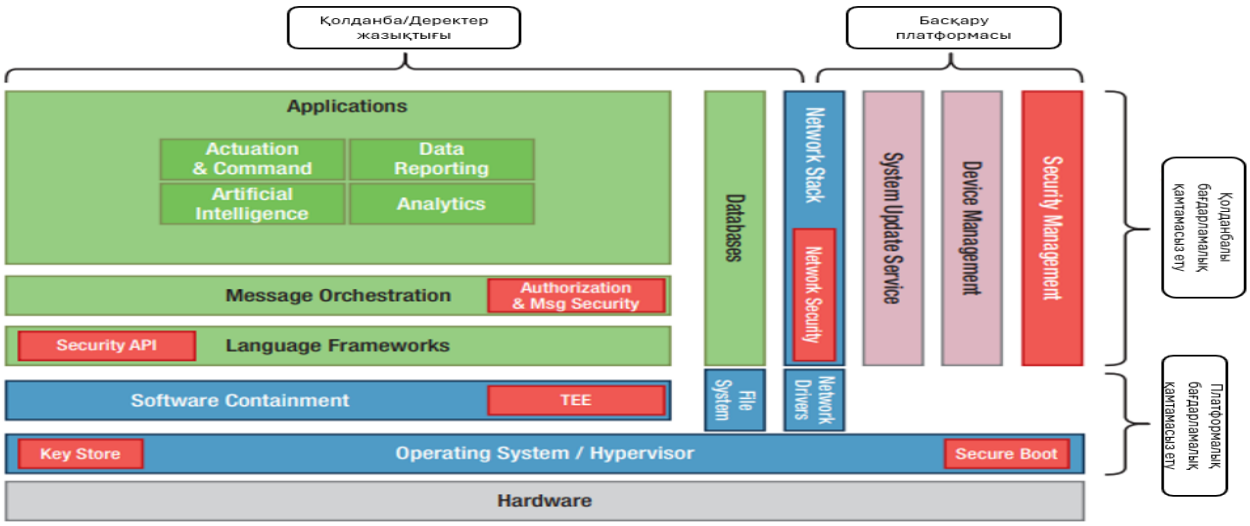
Бұл көптеген әртүрлі вертикалдардағы пайдаланушылар үшін жаңа мүмкіндіктер ашады. Мысалы, оны қауіпті ортадағы ауыр техниканы қашықтан басқару үшін пайдалануға болады, осылайша жұмысшылардың қауіпсіздігін арттырады. Төмен кідірістің арқасында ол қашықтағы операцияларды қосу арқылы денсаулық сақтау қызметіне қолжетімділікті жақсарта алады.

5G байланысы интеллектуалды көліктер мен көлік инфрақұрылымын болашақта қолдайтын болады. 5G көптеген салаларда инновацияларды алға жылжытатыны және IoT шешімдерінің экономикамыздың ажырамас бөлігіне айналуы үшін платформа беретіні анық.

2.2 IoT платформасындағы қауіпсіздік құрылыс блоктары

IoT бағдарламалық қамтамасыз етуінің қауіпсіздік құрылыс блоктарын егжей-тегжейлі қарастыру барысында құрылыс блогының әрбір құрамдас бөлігі үшін мәтінмәнді орнату және олардың IoT құрылғысын жасау үшін қалай үйлесетінін орнату үшін архитектуралық диаграмма өте маңызды рөл ойнайды. 2.4-суретте төрт жүйеге бөлінген, олардың әрқайсысында әртүрлі мақсаттарға арналған бағдарламалық құрал бар. Вертикалды орналасқан, ол платформалық

бағдарламалық қамтамасыз ету, яғни платформалық ортаны жасайтын бағдарламалық қамтамасыз ету және қолданбалы бағдарламалық қамтамасыз ету, яғни жүйенің платформалық әрекетін жасайтын бағдарламалық қамтамасыз ету болып бөлінеді. Ал, көлденең орналасқан, ол жүйені басқарумен айналысатын басқару жазықтығы мен басқаруға қатысы жоқ барлық басқа нәрселерді қамтитын (қолданба/деректер) жазықтығы.



2.4-сурет – IoT платформасының диаграммасы

Аппараттық құралдың тікелей үстінде операциялық жүйе/гипервизор элементі орналасқан, ол жүйелік бағдарламалық құрал болып табылады. Басқарушы аппараттық құрал коммерциялық немесе ашық бастапқы операциялық жүйе болуы мүмкін немесе бағдарламалық жасақтаманың қалған бөлігі іске қосылуы үшін бір немесе бірнеше виртуалды аппараттық құрылғыларды жасайтын гипервизор болуы мүмкін.

Бағдарламалық құралды шектеу элементі міндетті емес, бірақ жүйеге қосылса, ол контейнерлер және сенімді орындау орталары (TEE) сияқты технологияларды қамтиды. Бұл қосымша оқшаулау қабаты артықшылықтарды азайту және қолданбалар арасындағы күтпеген өзара әрекеттесуді басқару арқылы қауіпсіздікті жақсартады. Контейнерлер де, гипервизорлармен виртуализация да қамтуды қамтамасыз етеді. 1.9-суретте платформалық бағдарламалық құрал құрамдастарының арасында қиылысатын екі құрамдас көрсетілген: файлдық жүйе және желі драйверлері. Олар стектің қолданбалы бөлігі мен платформа бағдарламалық құралы арасындағы байланысты түсінуге көмектесу үшін диаграммада көрсетілген.

Платформалық бағдарламалық жасақтамадан қолданбалы бағдарламалық жасақтамаға көшу, біз басқару жазықтығына қараймыз. Басқару жоспарының бағдарламалық құралы қауіпсіздікті басқарудан, құрылғыларды басқарудан және жүйені жаңарту қызметінен тұрады. Ол сонымен қатар желілік стекті қамтиды. Желілік стек көбінесе жүйелік бағдарламалық құралға немесе операциялық жүйенің бір бөлігіне кіреді. Дегенмен, біздің мақсаттарымыз үшін оны

операциялық жүйеге қосу оны жасырады және IoT жүйелері үшін маңыздылығын төмендетеді. Желілік стек ерекше назар аударуды қажет етеді, өйткені ол жүйені басқа құрылғылармен байланысуға мүмкіндік береді, жүйені Интернет заттары құрылғысына айналдырады. Сонымен қатар, желілік стек IoT жүйелеріне шабуылдардың көпшілігі үшін кіру нүктесі болып табылады. Ол қолданбалы/деректер жазықтығы мен басқару жазықтығының екеуін де қамтиды, өйткені оны екі тарап кеңінен қолданады. Ол байланыс протоколдарын және желілік интерфейстерді қамтиды. Желілік стек ішкі бөлімінде желіаралық қалқандар және енуді анықтау жүйелері (IDS) сияқты желілік стекті қорғауға қажетті бағдарламалық құрал элементтері талқыланады.

Қауіпсіздікті басқару – қауіпсіздікке қатысты басқару операцияларын орындайтын және қауіпсіздік процедуралары мен басқару элементтерін орындауда қолданылатын басқару бағдарламалық құралы. Қауіпсіздікті басқару функционалдығы құрылғыны сәйкестендіру және аттестациялау, кілттерді тарату және сертификаттарды басқару, кіруді басқару саясаты, журнал жүргізу ережелері, жүйені жаңарту қызметінің конфигурациясы мен сұрауы, сондай-ақ желілік қауіпсіздік саясаты, брандмауэрлер, вирус сканерлері және хосттың кіруді анықтау бағдарламалық құралын қамтиды. Көбінесе бұл функциялар құрылғыларды басқаратын нақты бағдарламалық құралдың бөлігі ретінде қосылады. Біздің көзқарасымыз қауіпсіздікті басқаруды басқа басқару функцияларынан ең аз артықшылықтар принципіне сәйкестікті баса көрсету үшін бөледі.

Қауіпсіздікті басқару мүмкіндіктері әкімшінің белсендіруі үшін артықшылықтың жоғары деңгейлерін және қосымша аутентификацияны талап етуі керек. Құрылғыны басқару қауіпсіздік бақылауының бөлігі болып табылмайтын барлық басқару функцияларын қамтиды. Бұған құрылғы күйін сұрау және басқару, платформаны қайта жүктеу/қайта іске қосу, журнал файлдарын тексеру және жүктеп алу (бірақ журнал файлдарын жою немесе бұл қауіпсіздікті басқару мүмкіндігі болғандықтан журнал жасауды тоқтату), қолданбаларды іске қосу, тоқтату және қайта іске қосу кіреді. , қолданбаларды конфигурациялау, дерекқорларды басқару және хабарлар кезегі мен бағдарламалық құралды басқару параметрлерін конфигурациялау.

Жүйені жаңарту қызметі басқару жазықтығының соңғы құрамдас бөлігі болып табылады. Бұл элемент қауіпсіздікті басқару (немесе кейбір платформаларда құрылғыны басқару) арқылы басқарылатынына қарамастан, ол әдетте жүйедегі қолданбалы бағдарламалық құрал мен орындау контейнерлерінен көбірек жаңарту үшін платформаға және операциялық жүйеге тән элементтерден тұрады. Жүйе мен құрылғының микробағдарламасына, жүктеу жүктеушілеріне және BIOS жаңартулары, әдетте, нұсқа тәуелділіктерін дұрыс үйлестіру және платформаны осындай құрамдастарды жаңартуға болатын күйге келтіруге мүмкіндік беретін арнайы бағдарламалық құрал мен қызметтерді қажет етеді.

Микробағдарламаны және құрылғыдағы сенімді бағдарламалық құралды жаңартуға жүйелік құқықтар күнделікті басқару функцияларынан қатаң түрде

бөлінуі керек. Қолданба/деректер жазықтығы IoT құрылғысының нақты әрекетін жасайтын бағдарламалық құралды қамтиды. Бұған тілдік платформалар, хабарламалар оркестрі, дерекқорлар және қолданбалардың өздері кіреді. Бұл элементтерді талқылау шектеулі, өйткені біз осы элементтердің аппараттық қауіпсіздік мүмкіндіктерін пайдаланатын бөліктеріне ғана назар аударамыз.

Тілдік платформаларда қолданбалы бағдарламалық құрал пайдаланатын кітапханалар мен қызметтер бар. Мысалдар: Java-дағы Android платформасы, Node.js кітапханалары және JavaScript-тегі Sails платформасы. Хабарламаларды басқару бір платформадағы қолданбаларға байланысуға мүмкіндік береді, бірақ одан да маңыздысы желі арқылы машинадан машинаға (M2M) байланысты қамтамасыз етеді. MQTT, хабарламалар кезегі және Кафка сияқты жариялаушы-жазылу (pub-sub) платформалары сияқты хаттамалар хабарламаларды басқару шелегіне түседі.

Деректер базалары IoT жүйелерінің маңызды бөлігі болып табылады, өйткені олар IoT жүйелері арқылы жасалатын, өңделетін және тұтынылатын деректерді сақтауға, корреляцияға және өңдеуге мүмкіндік береді.

2.3 Интернет заттарының (IoT) деректер моделін және жүйелік абстракцияларды талдау

IoT платформалары қолданбалар платформа деректерімен тікелей әрекеттесу үшін қолданба деңгейіндегі абстракцияны анықтайды. Интернет заттарының (IoT) деректер моделі – құрылғыларды, сенсорларды, жетектерді және Интернетке қосылған басқа нысандарды сипаттайтын деректер құрылымы. Ол құрылғылар мен басқа жүйе құрамдастары арасында ақпаратты ұйымдастыру және тасымалдау жолдарын қамтамасыз етеді. IoT деректер моделінің кейбір негізгі элементтері:

Құрылғылар: бұл Интернетке қосылуға болатын физикалық нысандар, мысалы, сенсорлар, жетектер, смарт құрылғылар және т.б.

Деректер: бұл IoT құрылғылары жинайтын және тасымалдайтын ақпарат. Бұл температураны, ылғалдылықты, қысымды, заттардың орналасуын және т.б. өлшеулер болуы мүмкін.

Протоколдар: бұл құрылғылар мен басқа желі құрамдастарының деректермен алмасу жолын анықтайтын стандарттар мен конвенциялар. Мысалы, деректерді беру хаттамалары TCP/IP, MQTT, CoAP және т.б.

Бұлттық қызметтер: бұл IoT құрылғылары жинаған деректерді өңдеуге, талдауға және сақтауға арналған бұлтта ұсынылатын платформалар мен қызметтер.

Аналитика: бұл пайдалы ақпаратты алу, трендтерді анықтау, оқиғаларды болжау және т.б. үшін IoT деректерін талдау процесі.

Басқару жүйелері: бұл IoT құрылғыларын басқаруға, олардың күйін өзгертуге және алынған ақпарат негізінде белгілі бір әрекеттерді орындауға

арналған бағдарламалық және аппараттық құралдар. IoT жүйесінің абстракциялары көбінесе мыналарды қамтиды:

Қабаттар: IoT компоненттерін құрылғы деңгейі, желілік деңгей, қолданбалы деңгей және т.б. сияқты әртүрлі деңгейлерге ұйымдастыруға болады.

Модельдер: Модельдер құрылғылардың, деректердің және IoT жүйесінің басқа құрамдастарының абстрактілі көріністері болып табылады, бұл оларды түсінуді және басқаруды жеңілдетеді.

Қолданбалы бағдарламалау интерфейстері (API): API интерфейстері IoT жүйесінің әртүрлі құрамдас бөліктеріне деректер мен пәрмендер алмасуға мүмкіндік беретін байланысу жолдарын қамтамасыз етеді.

Бағдарламалық қамтамасыз ету: бұл IoT құрылғыларымен жұмыс істеуге, деректерді өңдеуге және жүйені басқаруға арналған бағдарламалық қосымшалар мен қызметтер.

Бұл абстракциялар мен модельдер IoT жүйелерін жобалау, орналастыру және басқару үшін негізді қамтамасыз етеді, бұл оларды әзірлеушілер мен әкімшілер үшін түсінікті және басқарылатын етеді.

Мысал ретінде қарастырсақ, температура сенсоры ағымдағы температураны (currTemp) және 24 сағаттағы орташа температураны (aveTemp) көрсете алады делік. Температура мәндерін Фаренгейт пен Цельсий бойынша көрсетуге болады.

Деректерді модельдеу тілдері схема анықтамасына сәйкес инфрақұрылым объектілерін егжей-тегжейлі сипаттау үшін қолданылады. Деректерді модельдеу тілдерінің мысалдарына XML (eExtensible Markup Language), JSON (JavaScript нысандарының ноталары), CBOR (Concise Binary Object Representation – екілік нысанның таңбашаларының көрсетілімі) және YANG (Yet Another Next Generation language – басқа келесі буын тілі) жатады. Деректер құрылымдарына қол жеткізу нақты анықталған желі интерфейстері арқылы жүзеге асырылады. Мысалы, CoAP төрт әдісті пайдаланатын REST моделінің интерфейсі болып табылады:

Платформа деректерімен әрекеттесу үшін GET, PUT, POST және DELETE. Жұп

RESTful интерфейсті анықтау тілдеріне RAML (Restful API

Модельдеу тілі) және Swagger. Рамалық түйін температура сенсоры, камера және электр шамы сияқты бірнеше нысандардан тұруы мүмкін.

Осы қарапайым, бірақ қуатты деректерді модельдеу құралдарын пайдалана отырып, IoT платформалары қосылымды орнату, маршруттау, пакетті жіберу, желілік мекенжайды аудару және т.б. негізінде жатқан желілік күрделіліктің көп бөлігін жасыра отырып, күрделі IoT жүйелерін сипаттай алады. Белгілі бір дәрежеде Интернет құрылымының дәрежесі of Things ақпаратты орталықтандырылған желілермен (ICN) салыстыруға болады.12 ICN аталған ақпарат желі архитектурасының орталық элементі болып табылатын желіні қайта елестетеді. Түйіндерге, желі топологиясына және протокол деңгейлеріне назар аударудың орнына, ICN деректердің түпкілікті байланысына назар

аударады. Деректер міндетті түрде соңғы нүктелерде орналаспайды, бірақ кэштеуге және желінің кез келген жерінде көшіруге болады. ICN сияқты, IoT инфрақұрылымының жоғарғы қабаты желінің деректерге бағытталған көрінісі болып табылады. Дегенмен, ICN-ден айырмашылығы, бар қабатты журналдар сақталады. Бұл қосымша күрделілік қосуы мүмкін, бірақ ол үлкен үйлесімділікті қамтамасыз етеді. Шынында да, ICN - IoT платформасының плагині ICN желісін бұрынғы желілермен қосудың ақылды тәсілі болып табылады. IoT хабарламаларын қорғау аутентификация, құпиялылық, құпиялылық және авторизация мақсаттарын жүзеге асыру үшін жан-жақты орындалуы керек. Әйтпесе, IoT матасының астындағы күрделілікті жасырудың артықшылығы оның орнына қауіпсіздік кемшіліктерін жасыруы мүмкін. IoT платформасын пайдаланатын IoT қолданбасы қауіпсіздік жүйе деңгейіндегі интерфейстер арқылы басқарылатынын білмеуі мүмкін. Интернет хаттамаларында көбінесе http үшін https және coap үшін coaps сияқты қауіпсіз балама болады, мұнда «s» қауіпсіздікті білдіреді. REST GET хабары coap үшін сияқты жұмыс істейді. Негізгі айырмашылық мынада: REST хабар алмасу протоколымен байланыстырылатын Көлік деңгейінің қауіпсіздігі (TLS) инфрақұрылымдық деңгей арқылы үйлестірусіз тікелей TLS ішкі жүйесіне беруге болатын тіркелгі деректерін (кілттер мен сертификаттар) пайдаланып қауіпсіз сеансты келіседі. Инфрақұрылымдық деңгей авторизацияға әсер етуді білмеуі мүмкін, бұл платформаның IoT қолданбалары үшін нақты қауіпсіздік жағдайын бұрмалауына әкелуі мүмкін. IoT платформалары түпкілікті қауіпсіздікке назар аудара отырып, дизайн мен іске асыруда әр түрлі болуы мүмкін.

3 Қауіпсіз байланысты қамтамасыз ету үшін IoT – тың WPA немесе WPA2 сияқты протоколдарын талдау

Осы WLAN қауіпсіздік саясатында сымды эквивалентті құпиялылық (WEP), Wi-Fi арқылы қорғалған қатынас (WPA – Wi-Fi Protected Access), WPA2 және WPA3 және WLAN аутентификациясы мен құпиялылық инфрақұрылымы (WAPI) болып табылады. Әрбір қауіпсіздік саясатында сымсыз қосылымды орнату үшін пайдаланылатын арна аутентификациясы, пайдаланушылар сымсыз желіге қосылу әрекеті кезінде пайдаланылатын пайдаланушы аутентификациясы және деректерді тасымалдау кезінде пайдаланылатын деректерді шифрлау сияқты бірқатар қауіпсіздік протоколдары болады. Осы WLAN қауіпсіздік протоколдары: WEP, WPA/WPA2, WPA3, PPSK, VAPI.

Осылардың аталған қауіпсіздік протоколдарының ең көп қолданыста болатын және танымал протокол WPA/WPA2. WPA (Wi-Fi – Wi-Fi Protected Access) және WPA2 сымсыз желілер үшін өте танымал қауіпсіздік стандарттары болып қала береді. Олардың танымал болуының негізгі себептері:

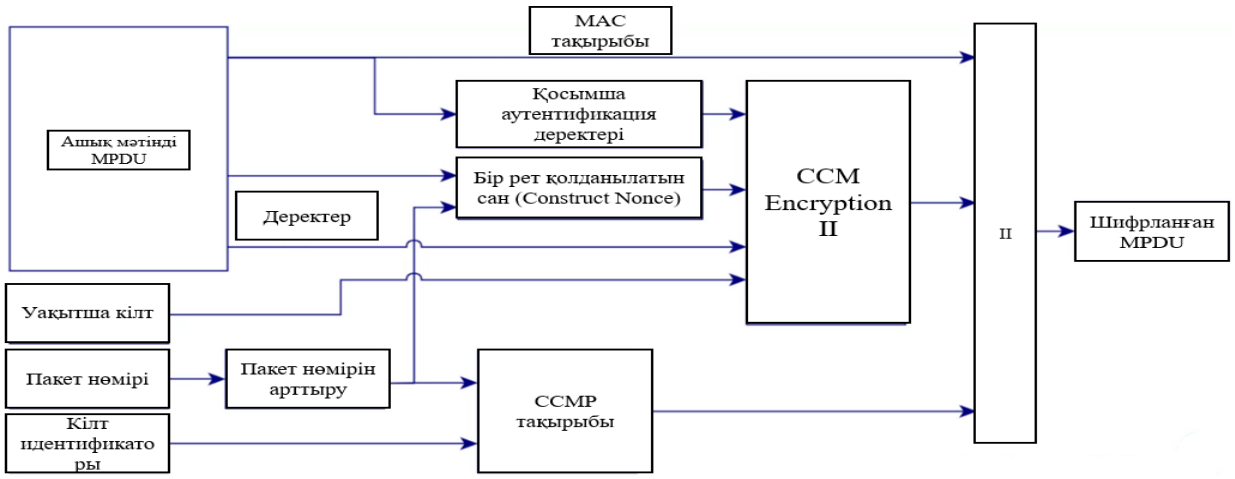
Кең таралған қабылдау және қолдау: WPA2, әсіресе, 2006 жылдан бері барлық заманауи Wi-Fi құрылғыларының қауіпсіздік стандарты болды. Бұл

әртүрлі өндірушілердің құрылғылары арасындағы үйлесімділіктің жоғары деңгейін қамтамасыз етеді.

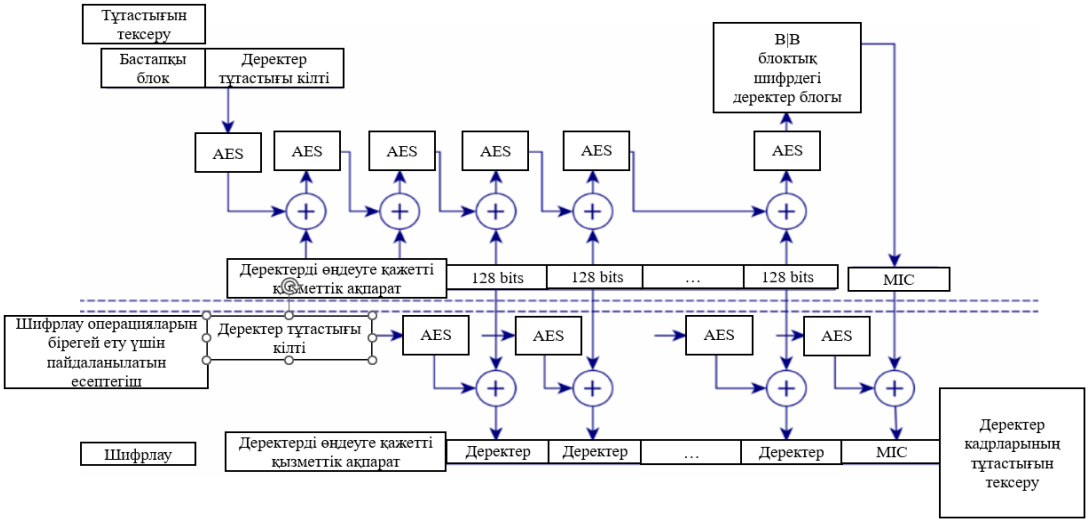
Орнату қарапайымдылығы: WPA/WPA2 жүйелерін соңғы пайдаланушылар үшін орнату оңай, бұл оларды үй және бизнес желілері үшін қолжетімді етеді. Көптеген құрылғылар пайдаланушыны қауіпсіздік конфигурациялау процесі арқылы бағыттайтын орнату шеберлерін ұсынады.

Жақсартылған қауіпсіздік: WPA2 күштірек AES (Advanced Encryption Standard) шифрлауын енгізу арқылы алдыңғы WPA нұсқасымен салыстырғанда қауіпсіздіктің маңызды жақсартуларын қамтамасыз етеді. Бұл оны құпия ақпаратты қорғау үшін тартымды таңдау жасайды.

Нормативтік және стандарттарға қойылатын талаптар: Көптеген қауіпсіздік стандарттары мен реттеуші органдар сымсыз желілер арқылы тасымалданатын деректерді қорғау үшін WPA2 пайдалануды талап етеді, әрі оны коммерциялық және институционалдық орталарда пайдалануды ынталандырады.



3.1-сурет – Wi-Fi қауіпсіздігінің WPA2 шифрлау схемасы



3.2-сурет – WPA2 шифрлауы

WPA2 сымсыз қауіпсіздікті айтарлықтай жақсартқанымен, оны IoT үшін қолайлы етпейтін кейбір мәселелер бар:

Конфигурациялау қиындығы: WPA2 конфигурациялау кейбір IoT құрылғылары үшін қиын болуы мүмкін, әсіресе оларда пайдаланушы интерфейсі болмаса.

Ресурсты тұтыну: WPA2 шифрлауы және аутентификациясы кейбір IoT құрылғыларында жетіспеуі мүмкін маңызды есептеу ресурстарын қажет етеді.

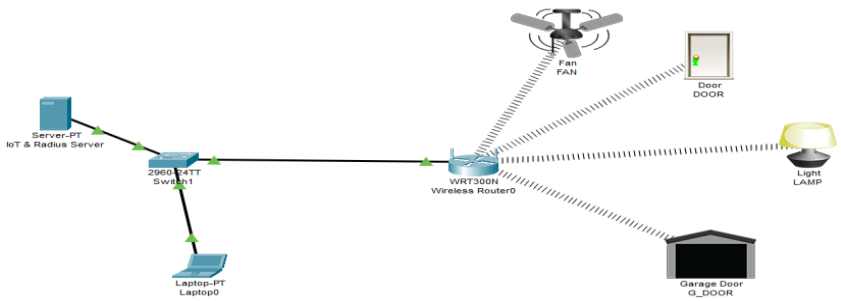
Осалдықтар: жақсартуларға қарамастан, WPA2 кейбір осалдықтарға сезімтал, мысалы, KRACK (Кілтті қайта орнату шабуылдары), бұл шабуылдаушыларға Wi-Fi арқылы тасымалданатын деректерді ұстауға мүмкіндік береді.

Оның танымалдығына қарамастан, соңғы жылдары белгілі осалдықтар, соның ішінде WPA2-ге KRACK шабуылдары бар. Бұл WPA3-тің дамуына әкелді, ол қауіпсіздік мүмкіндіктерінің жақсаруына және IoT құрылғыларына оңай қосылуға байланысты танымал бола бастады.

WPA3 жүйесіне көшу қазірдің өзінде басталды, бірақ көптеген құрылғылар мен желілер кеңінен қолдауға және бар жабдықты ауыстырудың дереу қажеттілігіне байланысты әлі де WPA2 пайдаланады. WPA3 WPA2-ні Wi-Fi қауіпсіздік стандарты ретінде қаншалықты жылдам ауыстыратынын уақыт көрсетеді.

3.1. CISCO бағдарламасындағы керек компоненттерді іске қосып, жүйені құру

Жобаның мақсатына сүйене отырып, қауіпсіз Wi-Fi желісі арқылы орталық маршрутизаторға әртүрлі IoT құрылғыларын (мысалы, смарт шамдар, термостаттар, қауіпсіздік камералары және басқа да автоматтандыру құрылғылары) қосатын смарт құрылғылары арқылы, WPA немесе WPA2 протоколдары деректерді шифрлау үшін пайдаланылатын және RADIUS сервері орталықтандырылған аутентификацияны басқаруды қосу арқылы біз жобамыздың үлгісін CISCO Packet Tracer бағдарламасы арқылы жүзеге асыра аламыз. Жобамыздың нақты үлгісі 3.1-суретте бейнеленген.

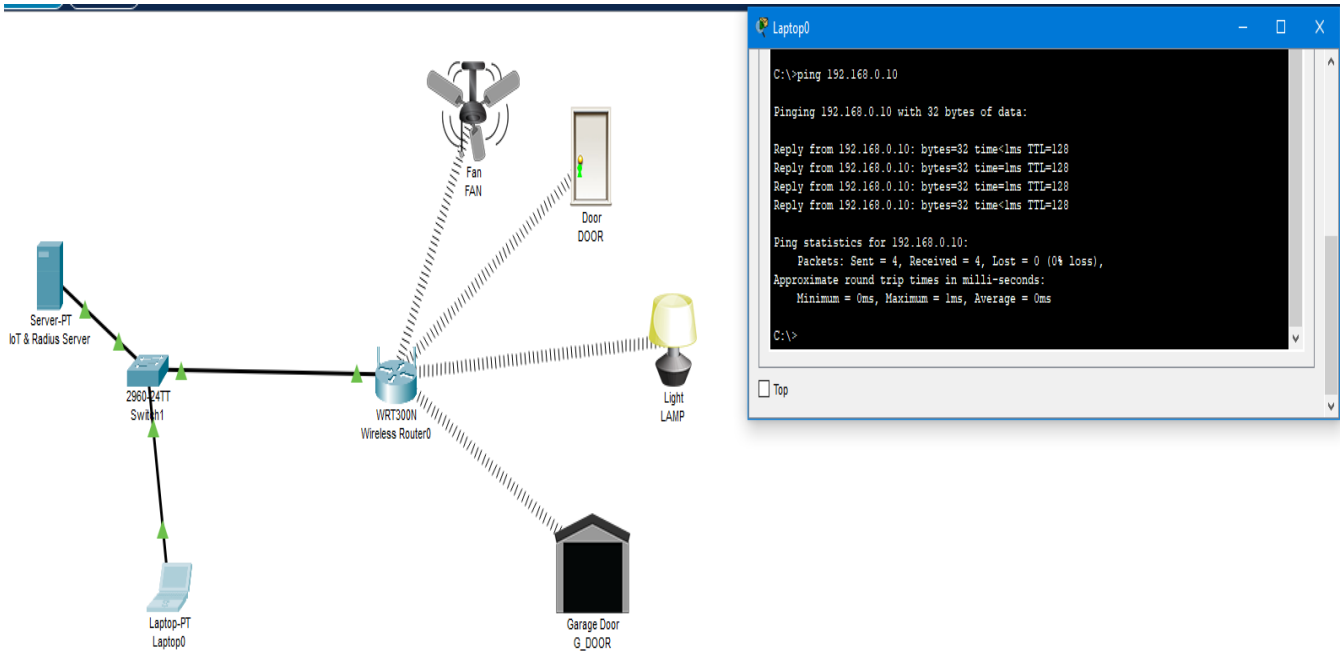


3.1-сурет – IoT құрылғыларымен байланысқан WPA/WPA2 қауіпсіздігінің байланыс жүйесі

Ал, 3.2-суретте Cisco жүйесіндегі ping пәрмесі арқылы, желілік операциялық жүйесінің, желілік құрылғы арасындағы қосылымды тексеру үшін, көрсетілген хостқа ICMP жаңғырық сұрау пакеттерін жіберетін және ICMP жаңғырық жауаптарын тыңдайтын функциясы арқылы жүйенің жағдайын анықтайтын командасының процессі көрсетілген, біздің жағдайда 0%. Демек, жүйе дұрыс құралған.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	IoT & ...	Wireless R...	ICMP		0.000	N	0	(edit)	
	Successful	IoT & ...	Laptop0	ICMP		0.000	N	1	(edit)	

3.2-сурет – Хаттама жіберу кезіндегі жүйенің статусы



3.3-сурет – Cisco IOS жүйесіндегі ping пәрмесі (біздің жағдайда 0% loss)

Жүйені құру үшін, бізге: 1x Server-PT, 2960-24TT Switch, WRT300N, Laptop/PC және IoT құрылғылар: FAN, Door, Lamp, Garage Door.

Server-PT: желілік қызметтерді басқаруға арналған сервер (DHCP, DNS және т.б.).

Cisco 2960-24TT коммутаторы: құрылғыларды қосуға арналған 24 портты қосқыш.

Linksys WRT300N: Wi-Fi байланысын қамтамасыз етуге арналған сымсыз маршрутизатор.

Ноутбук немесе ДК (дербес компьютер): желі ресурстарына қол жеткізуге арналған пайдаланушы компьютерлері.

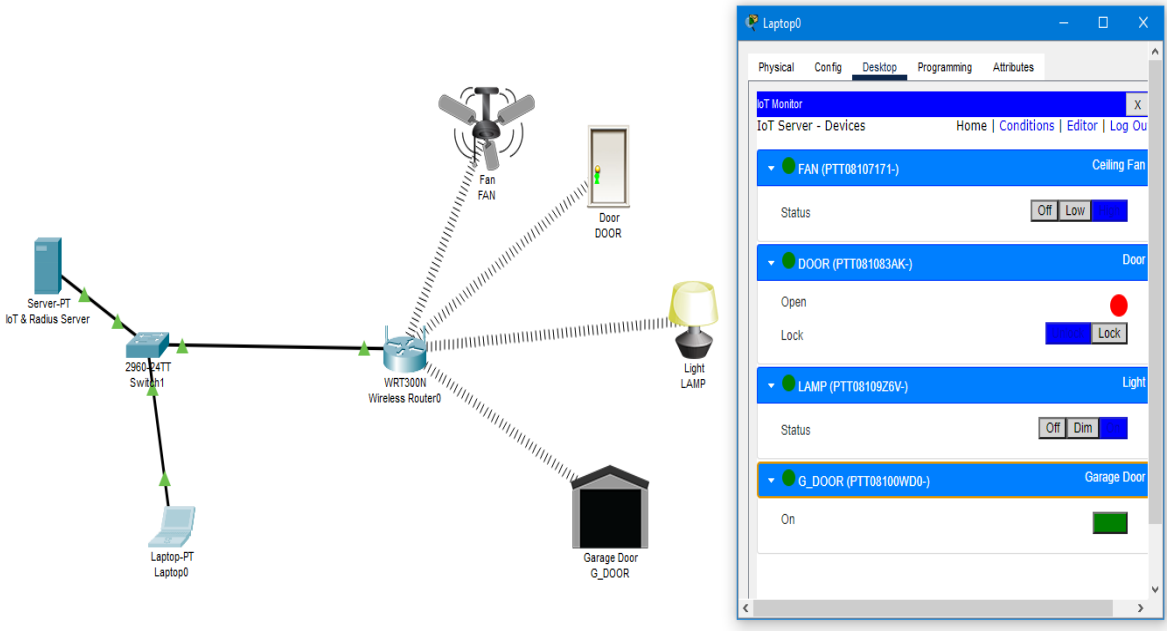
IoT құрылғылары: автоматтандырылатын желдеткіш, есік, шам және гараж есігі сияқты құрылғылар.

Cisco Packet Tracer бағдарламасында IoT Monitor мүмкіндігі симуляцияланған желіге қосылған заттардың интернеті (IoT) құрылғыларын басқаруға және бақылауға арналған. Оның нақты көрсетілген практикалық үлгі 3.3-суретте көрсетілген. Бұл құрал сенсорлар, смарт құрылғылар, жетектер және т.б. сияқты әртүрлі IoT құрылғыларының күйін және басқаруын көру үшін орталықтандырылған интерфейсті қамтамасыз етеді, бұл оны IoT қолданбаларын үйрену және әзірлеу контекстінде әсіресе пайдалы етеді. Мұнда Packet Tracer ішіндегі IoT мониторының негізгі мүмкіндіктері мен қолданбалары берілген:

Орталықтандырылған бақылау: IoT мониторы пайдаланушыларға барлық қосылған IoT құрылғыларының күйін бір жерде көруге мүмкіндік береді. Бұған қосылым күйлері, ағымдағы сенсор мәндері, жетек күйлері және басқа маңызды параметрлер кіреді.

Құрылғыны басқару: IoT мониторымен құрылғыларды олардың параметрлерін өзгерту немесе пәрмендерді жіберу арқылы қашықтан басқаруға болады. Мысалы, құрылғыларды қосуға немесе өшіруге, термостаттың температурасын реттеуге, шамдарды басқаруға және т.б.

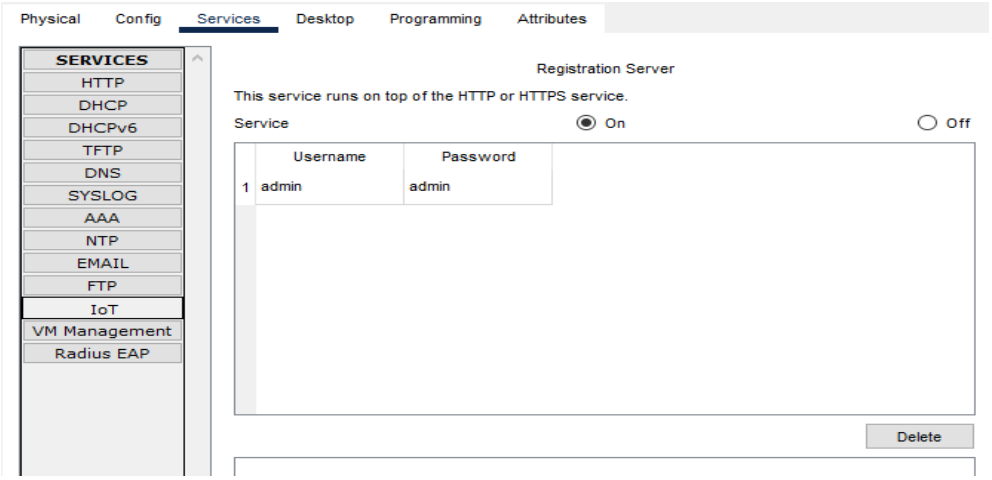
Бұл функция Packet Tracer-ді желілік технологияларды және IoT технологияларын әзірлеу және сынау үшін де қолайлы.



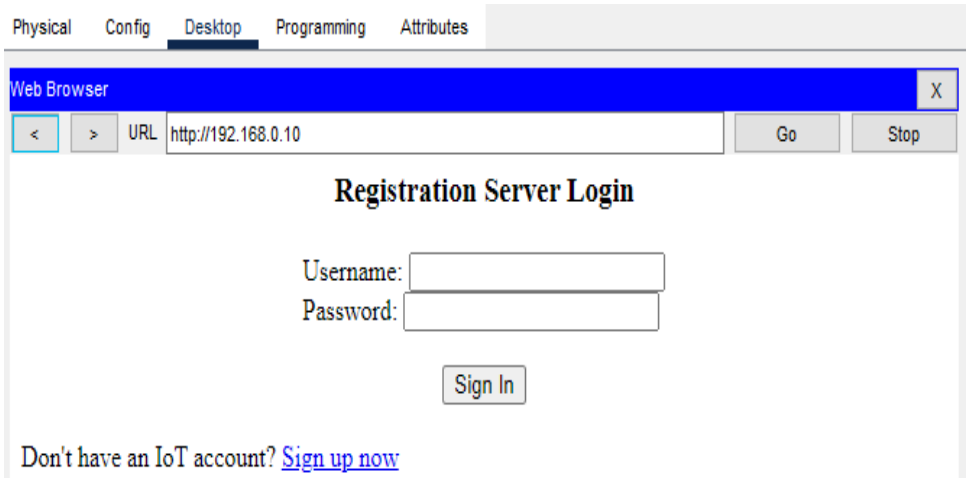
3.4-сурет – Жүйенің ДК арқылы немесе ноутбук арқылы өзгертулер енгізу мониторингі

Осы мониторингті іске қосу үшін, біз Server-PT желілік қызметтерді басқаруға арналған серверінде өзімізге «username»-пайдаланушы атын, «password»-пайдаланушының құпия сөзін енгіземіз, ол 3.4-суретте көрсетілген. Әрине әр құрылғыны басқару кезінде Web Browser панелінен бізге әр дайым осы

пайдаланушының аты мен құпия сөзін сұрайды. Себебі, ол тікелей Server-PT серверінен басқарылады, оның әкімші панеліне кіруі 3.5-суретте көрсетілген.

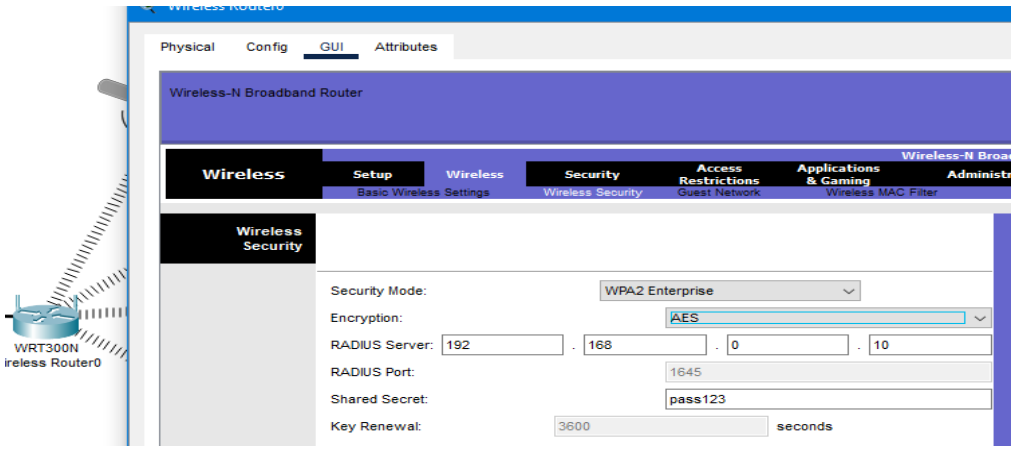


3.5-сурет – IoT серверіндегі әкімші панелін іске қосу, құпия сөзін беру

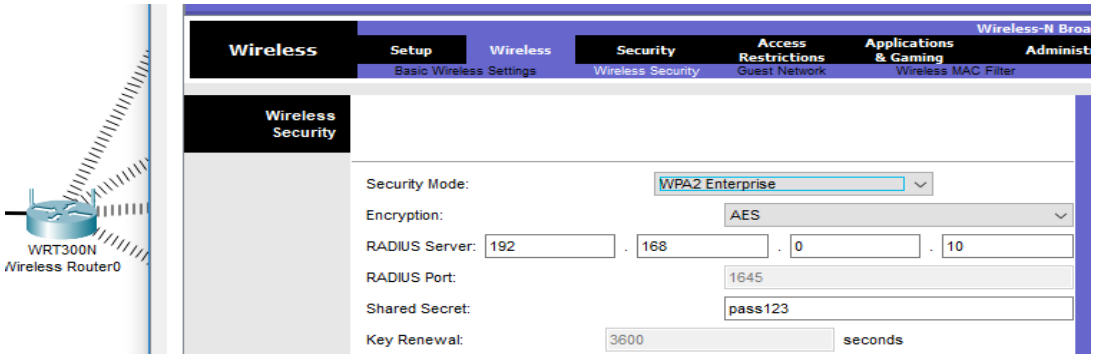


3.6-сурет – Әкімші панеліне кіру барысында құпия сөзді растау

Осы дипломдық жұмыста WRT300N маршрутизаторы қолданылуда. Ол, WPA2 шифрлау әдісін және 802.11n стандартын қолдау арқылы жаңа сымсыз құрылғылармен жақсырақ өнімділік пен үйлесімділікті қамтамасыз етеді. Негізгі шифр ретінде күшті AES блоктық шифры таңдалды. Аутентификация жүйесі WPA-мен салыстырғанда ең аз өзгерістерге ұшырайды. WPA сияқты, WPA2-де аутентификацияның екі нұсқасы бар: RADIUS серверінде аутентификациясы бар WPA2-Кәсіпорын және алдын ала орнатылған кілті бар WPA2-PSK. Біздің жағдайымызда RADIUS. Қосылу реті 3.5-3.6 суреттерінде нақты бейнеленген.

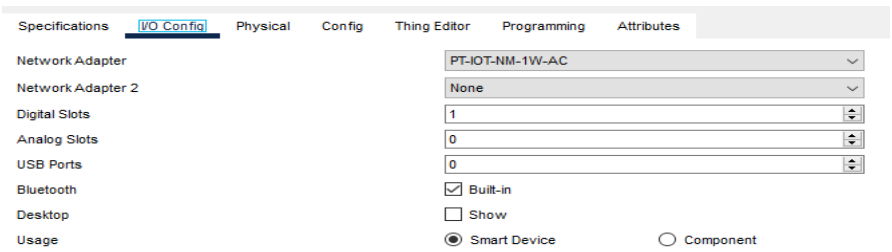


3.7-сурет – WPA2 қауіпсіздік протоколын қолданатын роутердің AES шифрлау әдісі

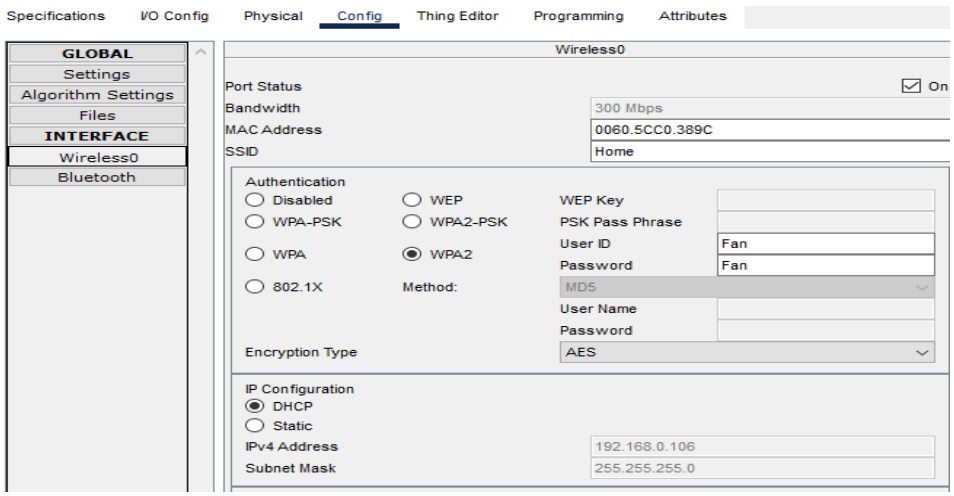


3.8-сурет – WPA2 қауіпсіздік протоколының іске қосылуы

Cisco Packet Tracer бағдарламасында PT-IOT-NM-1W-AC модулі симуляцияланған желідегі заттардың интернеті (IoT) құрылғыларын басқару және бақылау үшін пайдаланылатын желілік модульге жатады. Бұл модуль IoT құрылғылары мен маршрутизаторлар, қосқыштар және серверлер сияқты басқа желі құрамдастары арасындағы байланысты қамтамасыз етеді. Әр смарт құрылғыда 3.9-суреттегідей параметрлер орнатылған және 3.8-суретте бейнеленген желдеткіштің сипаттамаларында аутентификациясы (WPA2) және шифрлау әдісі (AES-Advanced Encryption Standard) таңдалынған.

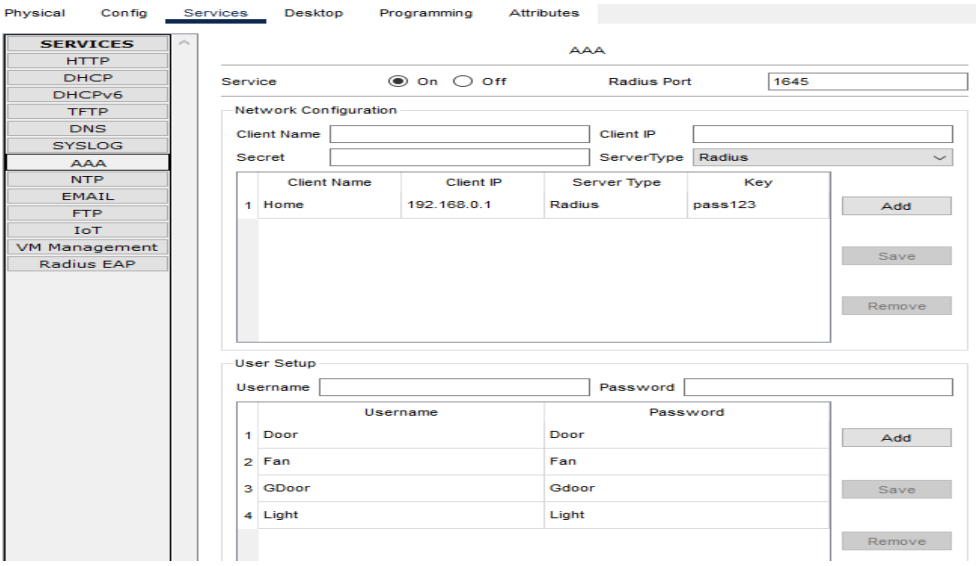


3.9-сурет – Смарт құрылғыларының кіріс-шығыс параметрлерін енгізілуі



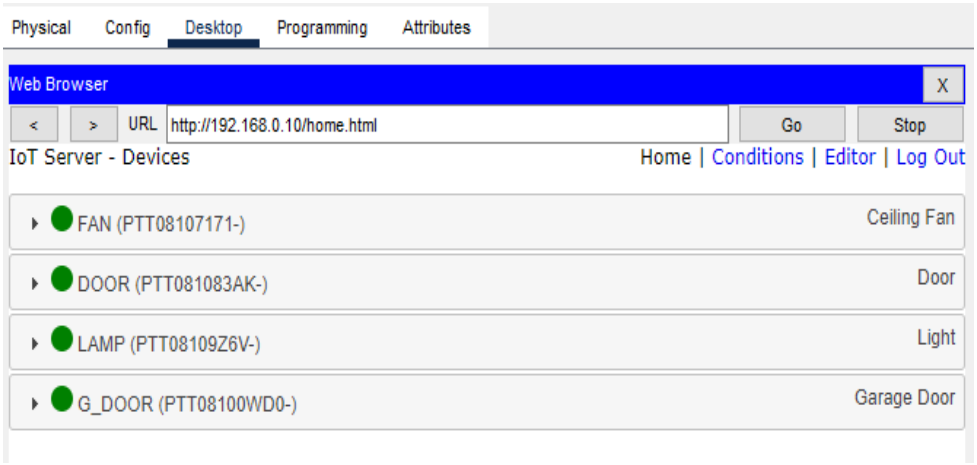
3.10-сурет – Смарт құрылғыларының WPA2 қауіпсіздігінің қосылынуы

Cisco Packet Tracer бағдарламасында сервердегі AAA (аутентификация, авторизация және есепке алу) панелі желілік инфрақұрылымдағы аутентификация, авторизация және есепке алу процестерін имитациялауға және басқаруға мүмкіндік береді. AAA желі қауіпсіздігінің маңызды құрамдас бөлігі болып табылады және ресурстарға қол жеткізуді басқару, сондай-ақ пайдаланушының әрекетін бақылау үшін нақты әлемдегі желілерде кеңінен қолданылады. Біздің жағдайда әр смарт құрылғы LAN байланысында роутердің 192.168.0.1 IP адресіне тікелей қосылымы болғандықтан, сәйкесінше керек енгізулерді жүктеп, сервер байланысының типін таңдап оған құпия сөзін енгіземіз. Осы орындалу тәсілін 3.11-суреттен байқауға болады.



3.11-сурет – IoT серверінің AAA параметріндегі енгізулер өрісі

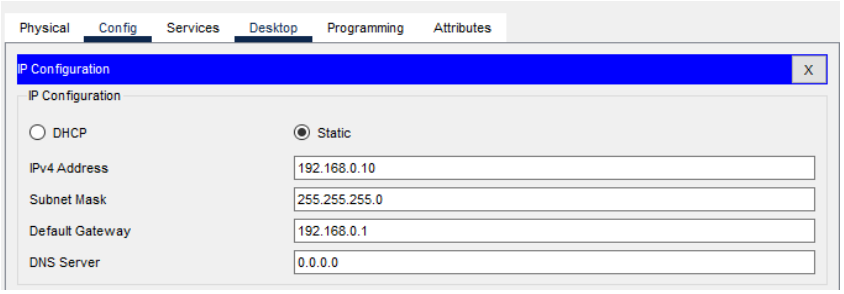
Осы смарт құрылғыларды басқару кезінде, біз ол құрылғыларға тек қол жеткізумен шектелмейміз. Біз оның күйін өзгертіп немесе қолданыстан да өшіре аламыз. Үлгі 3.12 және 3.13-суретте көрсетілген.



3.12-сурет – Смарт құрылғылар панелі

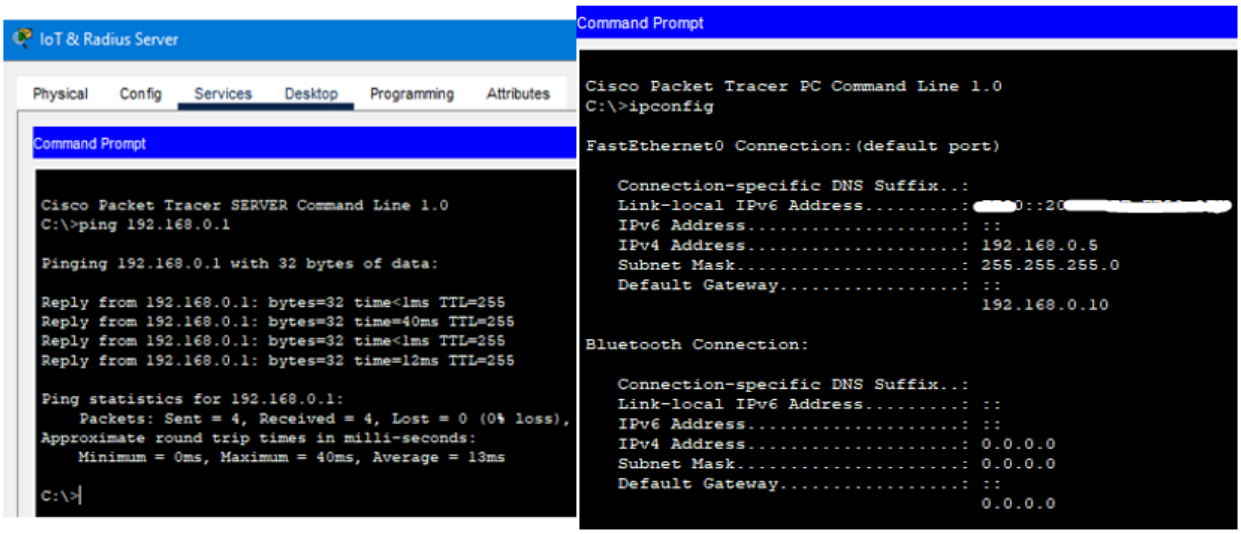
3.13-сурет – Смарт құрылғылар панелі, олардың күйін өзгерту мүмкіндіктері

Cisco Packet Tracer бағдарламасында "Server-PT" әртүрлі желі қызметтері мен функцияларын имитациялау үшін пайдаланылады және сервер құрылғысы болып табылады. Server-PT DHCP, DNS, HTTP, FTP, TFTP, SMTP, SNMP, AAA, NTP және басқалары сияқты қызметтердің кең спектрін қамтамасыз етеді, бұл оны желі жұмысын модельдеу және зерттеу үшін көп функциялы құрал етеді.



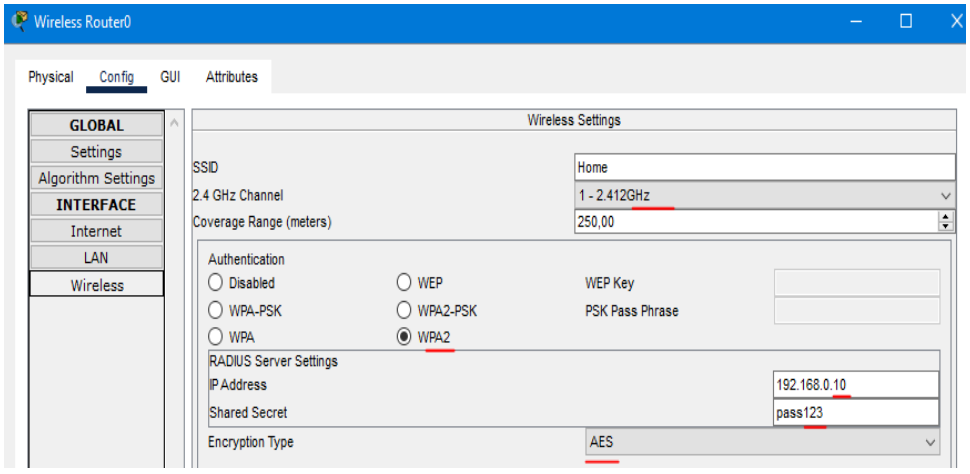
3.14-сурет – IoT серверінің IP адресі

Оған берілген IP адресі: 192.168.0.10. Оның байланысы әдепкі шлюзбен орнатылынған. Әдепкі шлюз(шлюз по умолчанию) — жергілікті желіден тыс деректер пакеттерін жіберу үшін компьютерлік желілерде қолданылатын құрылғы. Компьютер немесе смартфон сияқты құрылғы деректерді басқа желідегі мекенжайға жібергісі келсе, ол деректерді әдепкі шлюзге жібереді. Ал, бізде барлық IoT девайстары 192.168.0.1 IP адресіне тіркелгендіктен әдепкі шлюз WRT300N маршрутизаторы болады.



3.15-сурет – IoT серверінің басқа қосылымдарының күйінің немесе роутер/коммутаторлар мен IoT құрылғылардың арасындағы байланысы және ноутбук/ДК – дің нақты қосылыс порттары

Жалпы сервер мен маршрутизатор байланысы қарапайым «ping …(керек IP адресін жазсаңыз)» екі құрылғы арасындағы нақты байланысын, пакеттер жоғалуын біле аласыз. Біздің жағдайда, пакеттер жоғалуы - 0%. Орнатулар 3.13, 3.15-суреттерде. Сонымен қатар сымсыз роутердың байланыс параметрі, оған жазылған RADIUS серверінің IP адресін 3.14-суретте байқауға болады.



3.16-сурет – Қолданыстағы роутердің сымсыз байланыс параметрлері

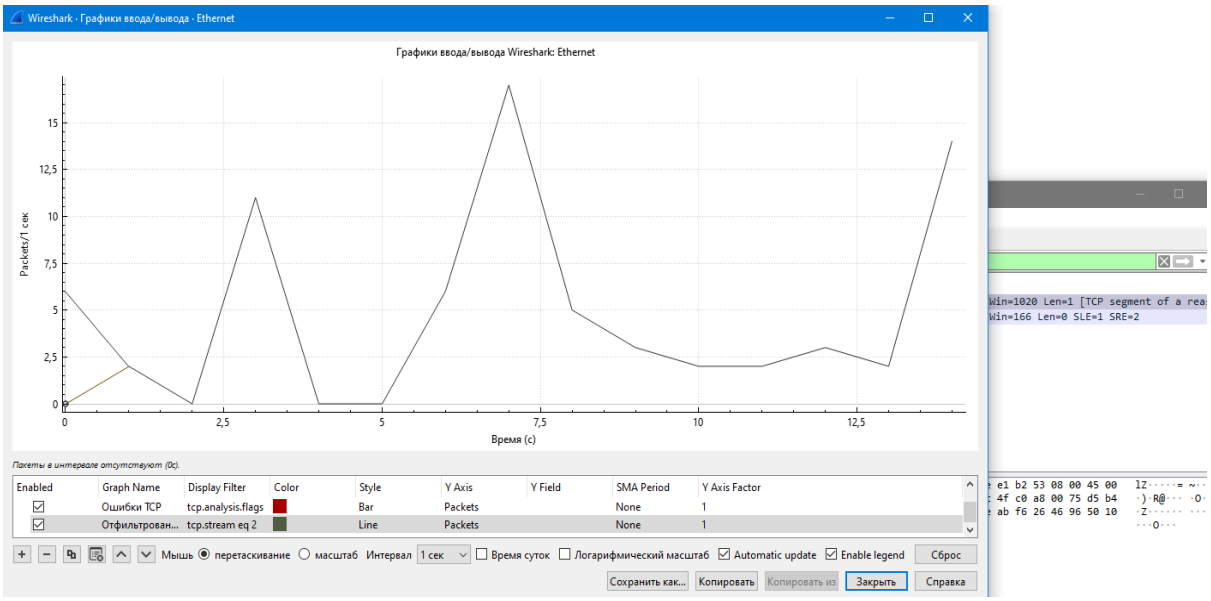
3.2 Wireshark бағдарламасының көмегімен желілік трафикті және байланыс хаттамаларын талдау, нақты уақыт режимінде желі арқылы пайдаланушыға өтетін барлық трафикті қарастыру

Wireshark - Ethernet компьютерлік желілеріне және басқаларына арналған трафик анализатор бағдарламасы. Графикалық пайдаланушы интерфейсі бар. Жоба бастапқыда Ethereal деп аталды, бірақ сауда белгілеріне байланысты жоба 2006 жылдың маусымында Wireshark деп өзгертілді[7].

Wireshark ұсынатын функционалдылық tcpdump функциясына өте ұқсас, бірақ Wireshark графикалық пайдаланушы интерфейсі және ақпаратты сұрыптау және сүзу үшін әлдеқайда көп опцияларға ие. Бағдарлама пайдаланушыға желі арқылы өтетін барлық трафикті нақты уақыт режимінде көруге мүмкіндік береді, желілік картаны промискую режиміне ауыстырады.

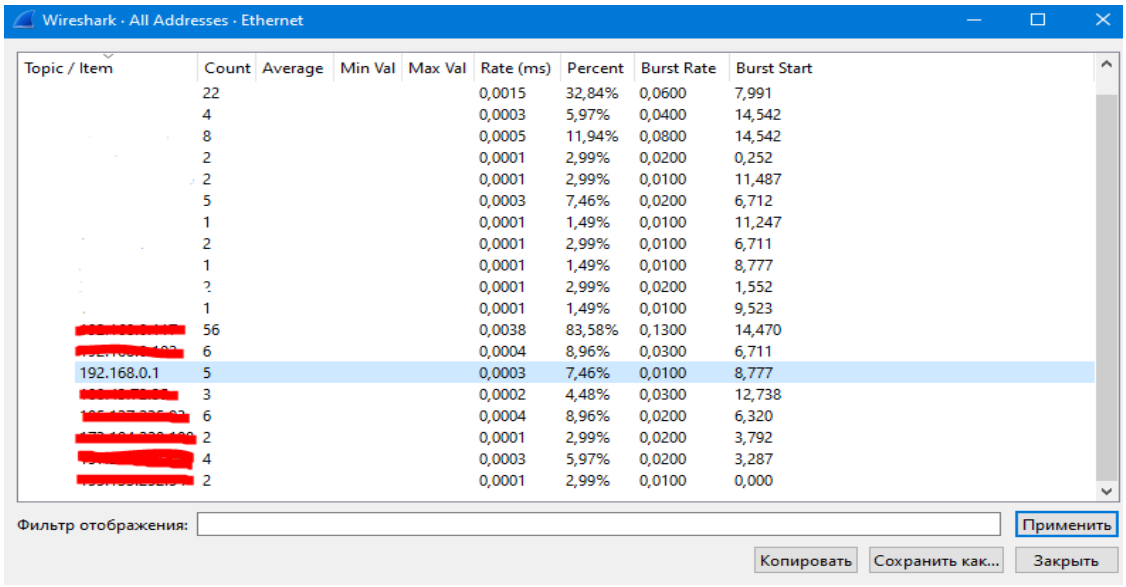
Бағдарлама тегін GNU GPL лицензиясы бойынша таратылады және графикалық интерфейсті жасау үшін кросс-платформалық GTK+ кітапханасын пайдаланады. GNU/Linux, Solaris, FreeBSD, NetBSD, OpenBSD, macOS, сонымен қатар Windows жүйесін қоса алғанда, UNIX-тәрізді жүйелердің көпшілігінің нұсқалары бар.

Wireshark — желілік хаттамалардың әртүрлі құрылымын «білетін» қосымша, сондықтан кез келген деңгейде әрбір протокол өрісінің мәнін көрсететін желілік пакетті талдауға мүмкіндік береді. «pcap» пакеттерді түсіру үшін пайдаланылғандықтан, деректерді тек осы кітапхана қолдайтын желілерден түсіруге болады. Дегенмен, Wireshark әртүрлі кіріс деректер пішімдерін өңдей алады, осылайша сіз басқа бағдарламалар түсірген деректер файлдарын ашып, түсіру мүмкіндіктерін кеңейте аласыз[10].



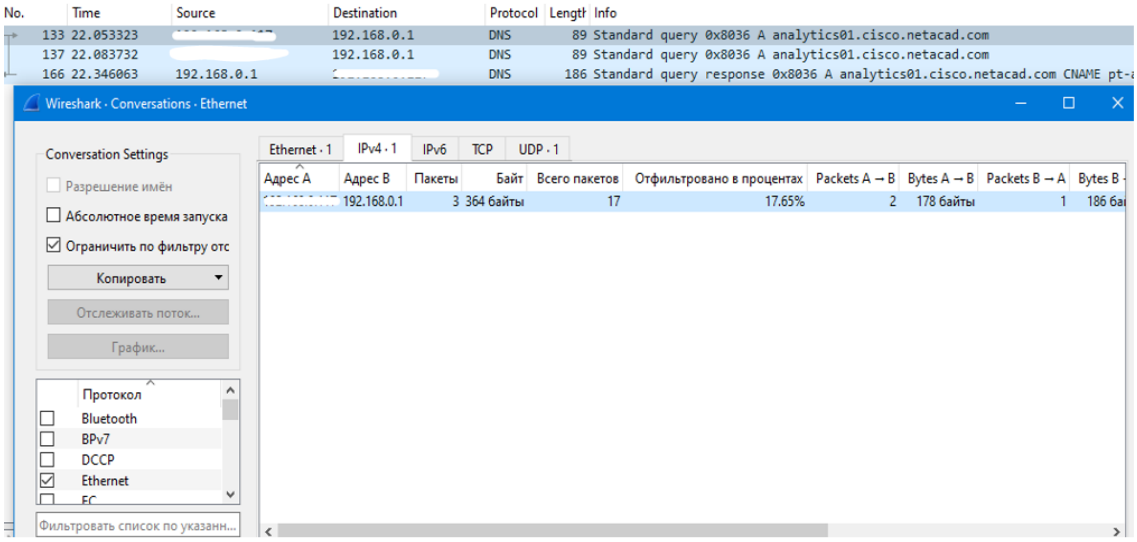
3.16-сурет – Wireshark бағдарламасы арқылы, кіріс/шығыс графигі уақыт бойынша деректер трафигінің күйі.

Жұмыстың барысында CISCO Packet Tracer мен Wireshark пен байланыстырғанда, бізге осы екі бағдарламаның Ethernet портындағы болып жатқан барлық ақпарат тамырларын көрсетеді.



3.17-сурет – Басып алынған пакеттермен байланысты барлық IP адресстер

Басып алу барысында біз CISCO бағдарламасында берілген IP адресін байқауға болады(3.17-сурет). Осы байланысты тікелей бақылау үшін «Conversation» терезесінен байқай аламыз. Оның расыменде CISCO бағдарламасы екенін білу үшін «Info» бөліміне назар аударып, білуге болады.

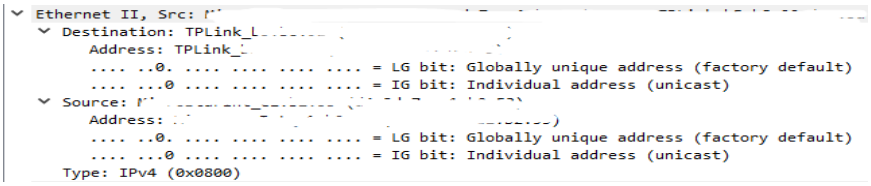


3.18-сурет – Басып алу барысындағы жүйенің Wireshark бағдарламасымен байланысы

Осы басып алу процессі нақты уақыттағы екі нүктенің байланысын көрсетеді ол А – менің, яғни ДК немесе ноутбуктың IP адресі және В – бағдарламада берілген IP адресі.

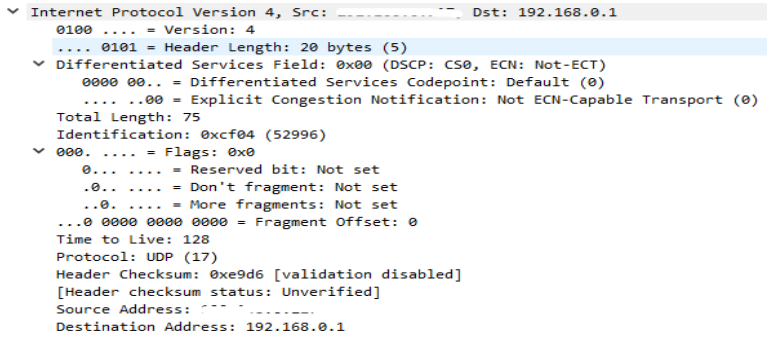
3.18-сурет – Басып алу барысындағы кадр саны және уақыты

Wireshark-та frame=137 түсірілген трафиктегі кадр нөмірін білдіреді. Wireshark желі сеансы кезінде ұстайтын әрбір деректер пакетіне кадр нөмірі ретінде белгілі бірегей реттік нөмір тағайындалады. Бұл нөмір шарлауды жеңілдету, талдау және трафикті түсіру журналындағы нақты пакеттерге сілтеме жасау үшін пайдаланылады. Сонымен қатар, басып алу барысында кадр ұзындығы көрсетілген ол 89 байт құрайды, яғни 89байт*8бит/байт=712бит.



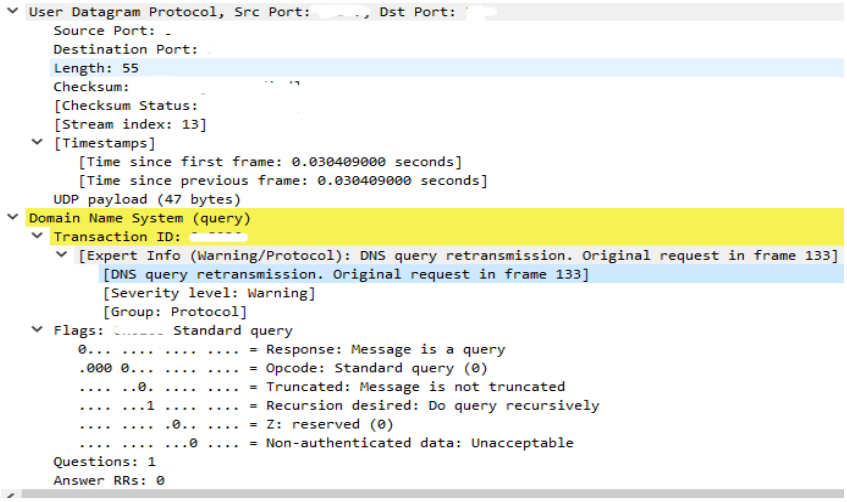
3.19-сурет – Басып алу барысындағы Ethernet портының кіріс шығысының анализі

Бұл суретте (3.19-сурет) практикада 2 роутер қолданғандықтан 2 роутердің байланыс процессі бейнеленілген бұл практикада күтпеген нәтиже еді, бірақ оны бейнелеп кету жөн.



3.20-сурет – «А» нүктесінен «В» нүктесіне дейінгі қолданатын протокол

3.20-суреттен IP-дің v4 типі қолдануда екенін, жету керек нүктесін, яғни IP-сін, ақпарат ұзындығын, жалпы ұзындығын байқауға болады.



3.21-сурет – Басып алу барысындағы протоколдың әр кадр санының жету уақыты

UDP (User Datagram Protocol) – Интернет протоколының стекіндегі негізгі транспорттық деңгей протоколдарының бірі. UDP TCP (Transmission Control Protocol) жүйесінде табылған сенімділікті, тапсырысты және ағынды басқару механизмдерін жою арқылы ең аз кідіріс пен төмен өңдеу шығындарын қамтамасыз етеді. Біздің жағдайда ол қолданыста және DNS туралы сәл ақпарат байқауға болады. DNS (Domain Name System) — адам оқи алатын домен атауларын IP мекенжайларына аударатын атау жүйесі, оларды желілік жабдық Интернеттегі компьютерлер мен ресурстарды анықтау және орналастыру үшін пайдаланады. Басқаша айтқанда, DNS күрделі сандық IP мекенжайларының орнына қарапайым домен атауларын пайдалануға мүмкіндік беру арқылы Интернетті пайдаланушыға ыңғайлы етеді. Ол дегеніміз, www.example.com сияқты браузерге домен атауын енгізген кезде құрылғы сайттың сәйкес IP мекенжайын білу үшін атау серверіне DNS сұрауын жібереді. Web Browser-дің жұмыс принципі тура сондай.

3.22-сурет – Жалпы басып алу барысындағы ретрансляция-желілік реле

Желілік релелік – бұл бір немесе бірнеше құрылғылар арқылы бір құрылғыдан екінші құрылғыға деректерді беру процесі. Бұл процесс желілік қамтуды кеңейтуде және оның ауқымдылығын арттыруда шешуші рөл атқарады. Реле OSI желі моделінің әртүрлі деңгейлерінде қолданылады және бірнеше түрлі техникалар мен технологияларды қамтуы мүмкін. Оның жұмыс істеу қалыпы «True» қалпында тұрғанын 3.22-суреттен байқай аламыз.

Осы жүйедегі бар ақпараттарды ескере отырып біз жүйенің арналардың пайдалану санын есептеп ала аламыз. Ең алдымен біз арналардың пайдалануының контекстіне тоқтала кетейік.

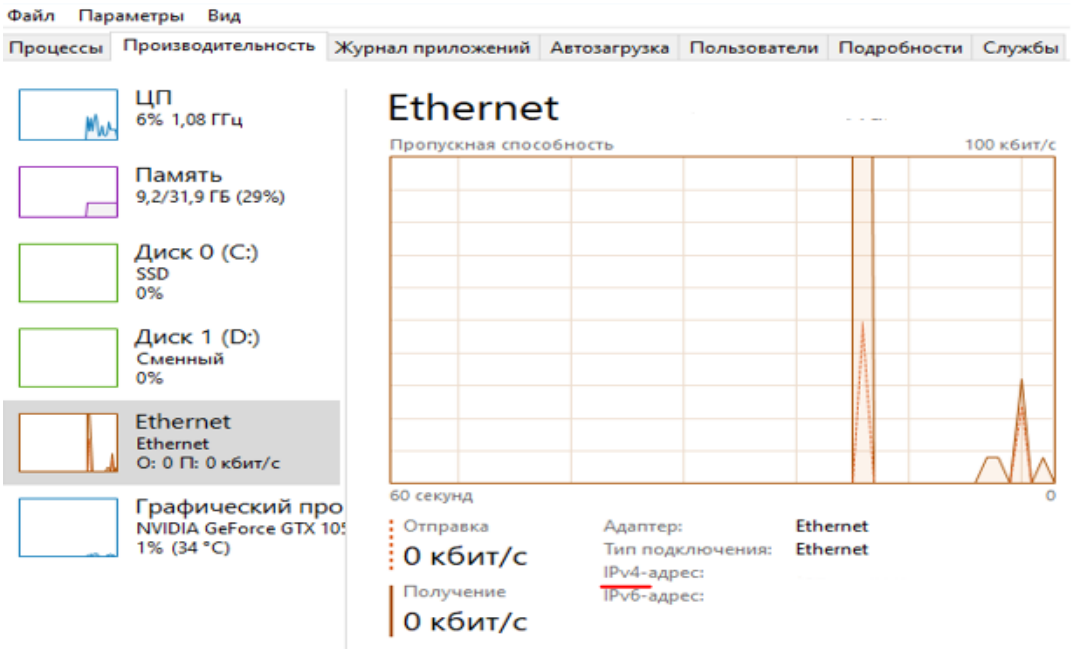
Желілік технологиялар интерьеріндегі арналарды пайдалану – бұл деректерді беру үшін жалпы желі арнасы сыйымдылығының қанша бөлігі пайдаланылатынын көрсететін көрсеткіш. Бұл параметр желінің тиімділігі мен өнімділігін бағалау үшін, сондай-ақ желілік инфрақұрылымды масштабтау мен жақсартуды жоспарлау үшін маңызды. Оның беріліс формуласы келесідей:

$$U = 100\% \times t1/t2 \qquad (3.1)$$

Utilization (U) or Efficiency=(Time taken to transmit frame)/(Total transmission time). (Prepared By: Dr. Mahmood Z. A. Ali)

Демек, Пайдалану (U) немесе тиімділік = (кадрды жіберуге кететін уақыт) / (жалпы жіберу уақыты) және «U = 100%× пайдаланылған өткізу қабілеті / оптикалық каб. орташа жылдамдығы» деп те есептеуге болады.

Егер, осы жұмыстағы мәндерді алсақ, бізге ең маңыздысы біздің Ethernet кабеліміздің өткізу қабілеті ол бізде 105.39 Мбит/с – қа тең оны мен өз ДК-нің тапсырмалар менеджерінен (диспетчер задач) анықтадым, оған буст орнатып, яғни, арнайы https://nls.kz/speedtest сайты арқылы максималды жылдамдығымды анықтадым. Бұл суретте (3.22-суретте) қызыл түспен белгіленген Wireshark бағдарламасында көрсетілген ДК-нің IP адресі жазылған.



3.23-сурет – Ethernet кабелінің максимал жылдамдығы

Осы анализаторда анықталған, үстіде айтылып кеткен өлшемдерді айтқанда бізге өзіміздің желілік арнаның пайдалануын анықтау үшін қолданыста болған 3 пакет, 364 байт деректер, кадр ұзындығы 89 байт және деректерді тасымалдаудың жалпы уақыты 22,053323с, керек IP-дан менің IP адресіме дейінгі 4864 бит/с – 178 байт және керісінше 5083 бит/с – 186 байт, және арнаның максималды өткізу қабілеті 105.39 Мбит/с.

Арнаның пайдалануын есептеу қадамдары:

1. Жалпы пайдаланылған өткізу қабілеттілігі = 5083 бит/с + 4864 бит/с = 9947 бит/с.

2. Біздің хабарламамыздағы сәйкес арнаның жалпы максималды сыйымдылығы 105,39 Мбит/с құрайды. Есептеуді жеңілдету үшін бұл мәнді секундына биттерге түрлендірейік:

105,39 Мбит/с = 105.39×10^6 бит/с.

3. Арнаның пайдалануы:

U = 100%× пайдаланылған өткізу қабілеті / оптикалық каб. орташа жылдамдығы = 100%×9947 бит/с / 105,39×10^6 бит/с = 0,00943828%

Бұл мән біздің арнамыздың пайдалануы шамамен 0,0094% құрайды, бұл жалпы арна өткізу қабілеттілігінің өте төмен пайдаланылғанын көрсетеді. Бұл арнаның өткізу қабілеттілігінің көп бөлігі қол жетімді және қазіргі уақытта пайдаланылмайтынын білдіреді.

ҚОРЫТЫНДЫ

Бұл дипломдық жұмысты қорытындылай келсек, осы IoT технологиясындағы үзіліссіз байланыс механизмінің қауіпсіздігіндегі WPA2 және AES маңыздылығы барлық жағдайындағы мүмкін болатын жағдайларды ескере отырып, көптеген талдаулар жүргізіліп, блоктар және де механизмдерінің байланыс күрделілігі айтылды.

Сонымен қатар, CISCO Packet Tracer мен Wireshark бағдарламаларын байланыстыра отырып, жүйені құрау және желілік трафикті, байланыс хаттамаларын талдау, нақты уақыт режимінде желі арқылы пайдаланушыға өтетін барлық трафик өлшенді.

Жалпы алғанда, барлық қойылған мақсаттар мен міндеттер орындалды.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1 Abdellah A.R. Deep Learning for IoT Traffic Prediction Based on Edge Computing.

2 Abdellah A.R., Artem V., Muthanna A., Gallyamov D., Koucheryavy A. // In: Vishnevskiy V.M., Samouylov K.E., Kozyrev D.V. (eds) Distributed Computer and Communication Networks: Control, Computation, Communications. DCCN 2020. Communications in Computer and Information Science, Springer,

3 Ali R. Abdellah, “IoT traffic prediction using multi-step ahead prediction with neural network,” /Ali R. Abdellah, Omar Abdul Kareem Mahmood, Alexander Paramonov, Andrey Koucheryavy // 2019 11th International Congress on Ultra Modern 140 Telecommunications and Control Systems and Workshops (ICUMT), Dublin, Ireland, 2019, pp. 1-4.

4 https://nls.kz/speedtest

5https://www.uomustansiriyah.edu.iq/media/lectures/5/5_2017_03_18!09_07_27_PM

6 Raza, S., Duquennoy, S., Chung, T., Yazar, D., Voigt, T., Roedig, U., 2011. Securing communication in 6LoWPAN with compressed IPSEC. Proceedings of IEEE DCOSS, 2011.

7 Raza, S., Voigt, T., Jutvik, V., 2012a. Lightweight ikev2: a key management solution for both compressed IPSEC and IEEE 802.15.4 security. IETF/IAB workshop on Smart Object Security.

8 https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/67134-wpa2-config.html

9 https://habr.com/ru/articles/735866/

10 https://www.wireshark.org/

ҒЫЛЫМИ ЖЕТЕКШІНІҢ ПІКІРІ

дипломдық жұмыска

Джахметов Асанәлі Ерланұлы

6В06201 «Телекоммуникация» білім беру бағдарламасы

Тақырыбы: IoT технологиясындағы үзіліссіз байланыс механизмінің қауіпсіздігін зерттеу

Жұмыстың мақсаты – кибер-кеңістіктегі заманауи қауіптерге төтеп бере алатын ауқымды және қауіпсіз жүйені әзірлеу. Осы мақсатқа жету үшін Wireshark бағдарламасы арқылы желілік трафикті түсіру және талдау, Cisco Packet Tracer жүйесінде желілік инфрақұрылымды модельдеу және әртүрлі шабуыл сценарийлері мен қорғаныс әдістерін қолдану арқылы жүйені сынау үшін пайдаланылды.

Жұмыстың нәтижелері қазіргі заманғы қауіпсіздік хаттамалары мен орталықтандырылған аутентификация әдістерін біріктіру жүйелердің қауіпсіздік деңгейін айтарлықтай арттыруға болатындығын көрсетеді. Жүйені енгізу, одан кейінгі тестілеу оның қол жеткізуді тиімді басқару және пайдаланушы деректерін қорғау қабілетін көрсетті.

IoT технологиясындағы үзіліссіз байланыс механизмінің қауіпсіздігіндегі WPA2 және AES маңыздылығы барлық жағдайындағы мүмкін болатын жағдайларды ескере отырып, көптеген талдаулар жүргізіліп, блоктар және де механизмдерінің байланыс күрделілігі айтылды.

Сонымен қатар, CISCO Packet Tracer мен Wireshark бағдарламаларын байланыстыра отырып, жүйені құрау және желілік трафикті, байланыс хаттамаларын талдау, нақты уақыт режимінде желі арқылы пайдаланушыға өтетін барлық трафик өлшенді.

Студент Джахметов Асанәлі дипломдық жұмысты жазу барысында жетекші нұсқаулығымен өз бетінше жұмыс істеу қабілетін көрсетті. Дипломдық жұмыс "95/А/ өте жақсы" деп бағаланды, ал студент ал Джахметов Асанәлі 6В06201 «Телекоммуникация» білім беру бағдарламасының “Ақпараттық және коммуникациялық технологиялар” саласының бакалавры дәрежесіне сай деп санаймын.

Ғылыми жетекші
ЭТжҒТ каф. қауымд. профессоры
PhD., докторы
_____ К.Н.Тайсариева
«10» 05 2024 ж.

К.И. САТБАЕВ АТЫНДАҒЫ ҚАЗАҚ ҰЛТТЫҚ ТЕХНИКАЛЫҚ ЗЕРТТЕУ УНИВЕРСИТЕТІ
КОММЕРЦИЯЛЫҚ ЕМЕС АКЦИОНЕРЛІК ҚОҒАМЫ

СЫН ПІКІР

дипломдық жұмыска

Джахметов Асанәлі Ерланұлы

6В06201 «Телекоммуникация» білім беру бағдарламасы

Тақырыбы: IoT технологиясындағы үзіліссіз байланыс механизмінің қауіпсіздігін зерттеу

Орындалды:

а) графикалық бөлім парақ;
б) түсініктеме бет.

ЖҰМЫСҚА ЕСКЕРТУ

Бұл зерттеу WPA/WPA2 протоколдарын және RADIUS сервері арқылы орталықтандырылған аутентификацияны қолдану арқылы қауіпсіздікті қамтамасыз етуге баса назар аудара отырып, Интернет заттары (IoT) технологиясындағы үздіксіз байланыс механизмінің қауіпсіздігін зерттеудің өзекті тақырыбына арналған. Киберқауіпсіздік қатерлерінің көбеюіне байланысты бұл зерттеу жеке деректерді қорғау және құрылғыларға қол жеткізуді бақылау қажеттілігіне бағытталған. Зерттеуге IoT аппараттық және бағдарламалық аспектілерін талдау, желі архитектурасын және құрылғылардың қауіпсіз өзара әрекеттесуін енгізу кіреді.

Заттар интернетін жүзеге асырудағы ерекше практикалық мәселе – өлшеу құралдарының максималды автономиясын қамтамасыз ету қажеттілігі, бұл бірінші кезекте сенсорларды электрмен жабдықтау мәселесін көрсетеді. Графикалық және мәтіндік материалдар МСТК талабына сәйкес жазылған. Бұл дипломдық жоба жоғарғы оқу орындарының талаптарына сай жеткілікті жоғарғы дәрежеде жазылған, алынған нәтижелер. Жұмыста грамматикалық қателер кездеседі. Ескерту ретінде, Wireshark бағдарламасының көмегімен желілік трафикті және байланыс хаттамаларын талданған, бірақ бір хаттамамен ғана жұмыс жасау дұрыс болар еді.

Студент Джахметов Асанәлі дипломдық жұмысты жазу барысында жетекші нұскаулығымен өз бетінше жұмыс істеу қабілетін көрсетті. Дипломдық жұмыс "95/A+/ өте жақсы" деп бағаланды, ал студент ал Джахметов Асанәлі 6В06201 «Телекоммуникация» білім беру бағдарламасының "Акпараттық және коммуникациялық технологиялар" саласының бакалавры дәрежесіне сай деп санаймын.

Рецензент
ҚазҰАЗУ, доктор PhD.,
қауымд.профессоры Әлібек Н.Б
«28» 05 2024 ж.

Университеттің жүйе администраторы мен Академиялық мәселелер департаменті директорының ұқсастық есебіне талдау хаттамасы

Жүйе администраторы мен Академиялық мәселелер департаментінің директоры көрсетілген еңбекке катысты дайындалған Плагиаттың алдын алу және анықтау жүйесінің толық ұқсастық есебімен танысканын мәлімдейді:

Автор: Джахметов Асанәлі Ерланұлы

Тақырыбы: IoT технологиясындағы үзіліссіз байланыс механизмінің қауіпсіздігін зерттеу

Жетекшісі: Кырмызы Тайсариева

1-ұқсастық коэффициенті (30): 3.1

2-ұқсастық коэффициенті (5): 1

Дәйексөз (35): 0.6

Әріптерді ауыстыру: 12

Аралықтар: 0

Шағын кеңістіктер: 1

Ақ белгілер: 0

Ұқсастық есебін талдай отырып, Жүйе администраторы мен Академиялық мәселелер департаментінің директоры келесі шешімдерді мәлімдейді :

☒ Ғылыми еңбекте табылған ұқсастықтар плагиат болып есептелмейді. Осыған байланысты жұмыс өз бетінше жазылған болып санала отырып, қорғауға жіберіледі.

☐ Осы жұмыстағы ұқсастықтар плагиат болып есептелмейді, бірақ олардың шамадан тыс көптігі еңбектің құндылығына және автордың ғылыми жұмысты өзі жазғанына қатысты күмән тудырады. Осыған байланысты ұқсастықтарды шектеу мақсатында жұмыс қайта өңдеуге жіберілсін.

☐ Еңбекте анықталған ұқсастықтар жосықсыз және плагиаттың белгілері болып саналады немесе мәтіндері қасақана бұрмаланып плагиат белгілері жасырылған. Осыған байланысты жұмыс қорғауға жіберілмейді.

Негіздеме:

28.05.2024
Күні

Кафедра меңгерушісі

Протокол

о проверке на наличие неавторизованных заимствований (плагиата)

Автор: Джахметов Асанәлі Ерланұлы

Соавтор (если имеется):

Тип работы: Дипломная работа

Название работы: IoT технологиясындағы үзіліссіз байланыс механизмінің қауіпсіздігін зерттеу

Научный руководитель: Кырмызы Тайсариева

Коэффициент Подобия 1: 3.1

Коэффициент Подобия 2: 1

Микропробелы: 1

Знаки из здругих алфавитов: 12

Интервалы: 0

Белые Знаки: 0

После проверки Отчета Подобия было сделано следующее заключение:

☒ Заимствования, выявленные в работе, является законным и не является плагиатом. Уровень подобия не превышает допустимого предела. Таким образом работа независима и принимается.

☐ Заимствование не является плагиатом, но превышено пороговое значение уровня подобия. Таким образом работа возвращается на доработку.

☐ Выявлены заимствования и плагиат или преднамеренные текстовые искажения (манипуляции), как предполагаемые попытки укрытия плагиата, которые делают работу противоречащей требованиям приложения 5 приказа 595 МОН РК, закону об авторских и смежных правах РК, а также кодексу этики и процедурам. Таким образом работа не принимается.

☐ Обоснование:

28.05.2024
Дата

Заведующий кафедрой

Протокол

о проверке на наличие неавторизованных заимствований (плагиата)

Автор: Джахметов Асанәлі Ерланұлы

Соавтор (если имеется):

Тип работы: Дипломная работа

Название работы: IoT технологиясындағы үзіліссіз байланыс механизмінің қауіпсіздігін зерттеу

Научный руководитель: Кырмызы Тайсариева

Коэффициент Подобия 1: 3.1

Коэффициент Подобия 2: 1

Микропробелы: 1

Знаки из здругих алфавитов: 12

Интервалы: 0

Белые Знаки: 0

После проверки Отчета Подобия было сделано следующее заключение:

☒ Заимствования, выявленные в работе, является законным и не является плагиатом. Уровень подобия не превышает допустимого предела. Таким образом работа независима и принимается.

☐ Заимствование не является плагиатом, но превышено пороговое значение уровня подобия. Таким образом работа возвращается на доработку.

☐ Выявлены заимствования и плагиат или преднамеренные текстовые искажения (манипуляции), как предполагаемые попытки укрытия плагиата, которые делают работу противоречащей требованиям приложения 5 приказа 595 МОН РК, закону об авторских и смежных правах РК, а также кодексу этики и процедурам. Таким образом работа не принимается.

☐ Обоснование:

18.05.2024
Дата

HR Казахстан

Марченя С.
проверяющий эксперт