ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ

әл-Фараби атындағы Қазақ ұлттық университетінің

ХАБАРЛАРЫ

ИЗВЕСТИЯ

НАЦИОНАЛЬНОЙ АКАДЕМИИ
НАУК РЕСПУБЛИКИ КАЗАХСТАН
Казахский национальный
университет имени аль-Фараби

N E W S

OF THE ACADEMY OF SCIENCES
OF THE REPUBLIC OF
KAZAKHSTAN
al-Farabi Kazakh National University

SERIES
PHYSICO-MATHEMATICAL

3 (343)

JULY – SEPTEMBER 2022

PUBLISHED SINCE JANUARY 1963

PUBLISHED 4 TIMES A YEAR

ALMATY, NAS RK

«ҚР ҰҒА Хабарлары. Физика-математикалық сериясы».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Меншіктеуші: «Қазақстан Республикасының Ұлттық ғылым академиясы» РҚБ (Алматы қ.). Қазақстан Республикасының Ақпарат және қоғамдық даму министрлігінің Ақпарат комитетінде 14.02.2018 ж. берілген **No 16906-Ж** мерзімдік басылым тіркеуіне қойылу туралы куәлік.
Тақырыптық бағыты: *ақпараттық коммуникациялық технологиялар сериясы.*
Қазіргі уақытта: *«ақпараттық технологиялар»бағыты бойынша ҚР БҒМ БҒСБК ұсынған журналдар тізіміне енді.*
Мерзімділігі: *жылына 4 рет.*
Тиражы: *300 дана.*
Редакцияның мекен-жайы: *050010, Алматы қ., Шевченко көш., 28, 219 бөл., тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Типографияның мекен-жайы: «Аруна» ЖК, Алматы қ., Мұратбаев көш., 75.

«Известия НАН РК. Серия физика-математическая».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Собственник: *Республиканское общественное объединение «Национальная академия наук Республики Казахстан» (г. Алматы).*
Свидетельство о постановке на учет периодического печатного издания в Комитете информации Министерства информации и общественного развития Республики Казахстан **No 16906-Ж** выданное 14.02.2018 г.
Тематическая направленность: *серия информационные коммуникационные технологии.*
В настоящее время: *вошел в список журналов, рекомендованных ККСОН МОН РК по направлению «информационные коммуникационные технологии».*
Периодичность: *4 раз в год.*
Тираж: *300 экземпляров.*
Адрес редакции: *050010, г. Алматы, ул. Шевченко, 28, оф. 219, тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Адрес типографии: ИП «Аруна», г. Алматы, ул. Муратбаева, 75.

News of the National Academy of Sciences of the Republic of Kazakhstan.
Physical-mathematical series.
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Owner: RPA «National Academy of Sciences of the Republic of Kazakhstan» (Almaty). The certificate of registration of a periodical printed publication in the Committee of information of the Ministry of Information and Social Development of the Republic of Kazakhstan **No. 16906-Ж,** issued 14.02.2018
Thematic scope: *series information technology.*
Currently: *included in the list of journals recommended by the CCSES MES RK in the direction of «information and communication technologies».*
Periodicity: *4 times a year.*
Circulation: *300 copies.*
Editorial address: *28, Shevchenko str., of. 219, Almaty, 050010, tel. 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Address of printing house: ST «Aruna», 75, Muratbayev str, Almaty.

NEWS OF THE NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 3, Number 343 (2022), 117-135
https://doi.org/10.32014/2022.2518-1726.142
УДК 004.49

Ж.С. Каженова[1*], Ж.Е. Кенжебаева[1], А.М. Прудник[2]

[1]С. Сейфуллин атындағы Қазақ агротехникалық университеті,
Қазақстан, Астана;

[2]Беларусь мемлекеттік информатика және радиоэлектроника
университеті, Белорусь, Минск.
E-mail: *zhkazhenova75@gmail.com*

MQTT (ТЕЛЕМЕТРИЯ ХАБАРЛАМАЛАРЫ КЕЗЕГІН ТАСЫМАЛДАУ) ХАТТАМАСЫНЫҢ ҚАУІПСІЗДІК МЕХАНИЗМДЕРІ

Аннотация. Заттар интернеті (IoT) соңғы жылдары зерттеулердегі өте өзекті тақырыпқа айналды. IoT желісіне жеңілдетілген болуы тиіс жаңа байланыс хаттамалары қосылды, мысалы, MQTT. Мақалада заттар интернетінің MQTT (Message Queue Telemetry Transport) хаттамасының ерекшеліктері, қолданылу нұсқалары және өзіндік сипаттағы процедуралары талқыланады. «Жариялаушы-жазылушы» принципі қарастырылады. MQTT хаттамасына әуел бастан тиімді қауіпсіздік функ циялары жетіспейді, себебі ол қарапайым мәтін түрінде пайда-ланушы аты мен құпия сөзге негізделген аутентификацияны орындайды. Сонымен қатар, тасымалдау деңгейінде толық шифрлау үшін SSL/TLS пайдаланылады, ал ол шектеулі ресурстары бар құрыл ғылар үшін жеңіл хаттама болып саналмайды. Егер IOT құрылғылары байланыстың үстеме шығындарын көтере алса, TLS әр уақытта қолданылуы керек, себебі, қауіпсіздік IOT әзірлемесінің ажырамас бөлігі болып табылады. Бұл мақалада біз кейінірек MQTT хаттамасына негізделген заттар интернеті (IoT) үшін жаңа жеңілдетілген аутентификация механизмін ұсыну мақсатында MQTT хаттамасының қауіпсіздік механизмдерін зерттейміз. Ол үшін MQTT хаттамасы арқылы екі IoT құрылғысы (Raspberry pi) арасында деректер алмасуды жүзеге асырдық. Құрылғы-

лардың бірі брокер және жазылушы, екіншісі жариялаушы рөлін атқарады. MQTT хаттамасында пайдаланушы аты және құпия сөзді қолданумен қорғалған арна және TLS хаттамасымен қорғалған арна жүзеге асырылуы мүмкін. MQTT хаттамасының қауіпсіздік механизмдеріне сәйкес, екі IoT құрылғысы арасында қорғалмаған арна арқылы ақпарат алмасу, пайдаланушы аты және құпия сөзді қолданумен қорғалған арна арқылы және TLS хаттамасымен қорғалған арна арқылы ақпарат алмасу кезіндегі арнаның өткізу қабілеттері өлшенді және салыстырылды.

Түйін сөздер: жариялаушы, жазылушы, заттар интернеті, қауіпсіздік, хаттама, MQTT, IoT құрылғылары.

Ж.С. Каженова[1*], Ж.Е. Кенжебаева[1], А.М. Прудник[2]

[1]Казахский агротехнический университет имени С. Сейфуллина,
Казахстан, Астана;
[2]Белорусский государственный университет информатики
и радиоэлектроники, Беларусь, Минск.
E-mail: *zhkazhenova75@gmail.com*

МЕХАНИЗМЫ БЕЗОПАСНОСТИ ПРОТОКОЛА MQTT (ТРАНСПОРТ ТЕЛЕМЕТРИИ ОЧЕРЕДИ СООБЩЕНИЙ)

Аннотация. Интернет вещей (IoT) в последние годы стал очень актуальной темой в исследованиях. В сети IoT включены новые коммуникационные протоколы, которые должны быть легкими, как, например, протокол MQTT. В статье рассматривается протокол MQTT (Message Queue Telemetry Transport) Интернета вещей, его особенности, варианты применения, характерные процедуры. Рассматривается принцип «издатель-подписчик». MQTT изначально не хватает эффективных функций безопасности, поскольку он выполняет аутентификацию на основе имени пользователя и пароля в виде простого текста. Кроме того, для полного шифрования на транспортном уровне используется SSL/TSL, который не считается облегченным протоколом для устройств с ограниченными ресурсами. Если устройства IOT могут нести накладные расходы на связь, TLS следует использовать каждый раз, так как безопасность является неотъемлемой частью разработки IOT.

В этом документе мы исследуем механизмы безопасности протокола MQTT с целью в дальнейшем представить новый облегченный механизм аутентификации для Интернета вещей (IoT) на основе протокола MQTT. Для этого мы реализовали обмен данными между двумя устройствами IoT (Raspberry pi) по протоколу MQTT. Один из усройств выступит в роли брокера и подписчика, другое будет выступать в роли издателя. Протокол MQTT может реализовать канал, защищенный именем пользователя и паролем, и канал, защищенный протоколом TLS. Согласно механизмам безопасности протокола MQTT, измерялась и сравнивалась пропускная способность канала при обмене информацией между двумя устройствами IoT по незащищенному каналу, по каналу, защищенному с помощью имени пользователя и пароля, и по каналу, защищенному протоколом TLS.

Ключевые слова: издатель, подписчик, Интернет вещей, безопасность, протокол, MQTT, устройства IoT.

Zh.S. Kazhenova[1*], Zh.E. Kenzhebayeva[1], A.M. Prudnik[2]

[1]S. Seifullin Kazakh Agrotechnical University, Kazakhstan, Astana;
[2]Belarusian State University of Informatics and Radioelectronics, Belarus, Minsk.
E-mail: *zhkazhenova75@gmail.com*

SECURITY MECHANISMS OF PROTOCOL MQTT (MESSAGE QUEUING TELEMETRY TRANSPORT)

Abstract. The Internet of Things (IoT) has become a very hot topic in recent years. The IoT network includes new communication protocols that should be lightweight, such as the MQTT protocol. The article discusses the MQTT (Message Queue Telemetry Transport) protocol of the Internet of Things, its features, applications, and characteristic procedures. The principle of “publisher-subscriber” is considered. MQTT initially lacks effective security features as it performs authentication based on a username and password in plain text. In addition, SSL/TSL is used for full transport layer encryption, which is not considered a lightweight protocol for devices with limited resources. If IOT devices can incur communication overhead, TLS should be used every time, as security is an integral part of IOT development.

In this paper, we explore the security mechanism of the MQTT protocol, with the aim of further introducing a new lightweight authentication mechanism for the Internet of Things (IoT) based on the MQTT protocol. To do this, we implemented data exchange between two IoT devices (Raspberry pi) using the MQTT protocol. One of the devices will act as a broker and subscriber, the other will act as a publisher. The MQTT protocol can implement a username and password protected channel and a TLS protected channel. According to the security mechanisms of the MQTT protocol, the channel throughput was measured and compared when exchanging information between two IoT devices over an insecure channel, over a channel protected with a username and password, and over a channel protected by the TLS protocol.

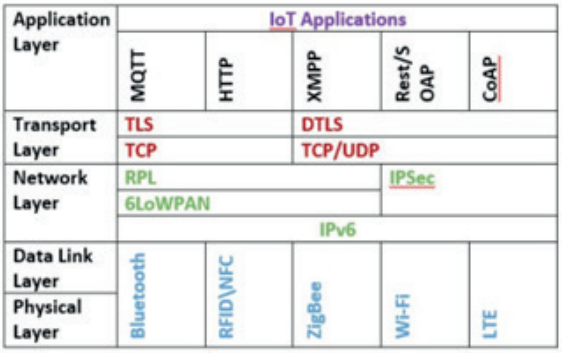
Key words: publisher, subscriber, Internet of Things, security, protocol, MQTT, IoT devices.

Кіріспе. Қазіргі кезде интернетке қосылған құрылғылардың және осы құрылғылар жасайтын деректер көлемінің жылдам өсуі байқалады. Кіріктірілген датчиктерді, сымсыз байланыстарды, процессорларды біріктіру арқылы заттар интернеті (IoT) желісін құруға болады. Заттар интернеті екі терминнен тұрады. Бірінші термин – бұл Интернет, ол миллиардтаған пайдаланушыларды, құрылғыларды, жүйелерді байланыстырады. Екінші термин – бұл интеллектуалды объектілерге жататын зат (Goyal т.б., 2018).

Заттар интернеті серпілісі деректер алмасу көрінісін өзгертті. Заттар интернетінің арқасында машинадан - машинаға (M2M) байланыс түрі пайда болды. Дегенмен, күнделікті заттарды интернетке қосу маңызды қауіпсіздік мәселелерін тудырады. Қауіпсіздік - заттар интернеті желілеріндегі басты мәселелердің бірі. IoT құрылғыларының көпшілігі ресурстарды және қуат тұтынуда шектеулі болғандықтан, сенімді қауіпсіздік механизмдерін енгізу оңай емес. Біздің алдыңғы мақаламызда IoT желілерінде кеңінен қолданылатын технологиялар мен стандарттарға сипаттама жасалған, сондай-ақ, қазіргі уақытта IoT жүйесінде қабылдау үшін қол жетімді ең танымал қауіпсіздік хаттамалары мен технологияларына шолу жасалған (Каженова т.б., 2022).

Ресурстарды тиімді пайдаланатын қолданбалы хаттамалар IoT ортасында хабар алмасу мен деректерді жеткізудің құрылыс блоктары болып табылады. Шектеулі қосымшалар хаттамасы (CoAP), кеңейтілетін хабар алмасу және қатысу хаттамасы (XMPP) және телеметрия

хабарламалары кезегін тасымалдау (MQTT) сияқты қосымша деңгей хаттамалары хабар алмасу мақсатында әзірленді. IoT хаттамалары стегінің жалпы тізімін 1-суретте көруге болады (Andy т.б., 2017).



1-сурет. IoT хаттамаларының стегі.

Қолданбалы деңгей соңғы түйіндер (IOT құрылғылары) мен желі арасындағы интерфейсті қамтамасыз етеді. Заттар интернетінде қолданылатын танымал хаттамалардың бірі - MQTT. MQTT (Message Queue Telemetry Transport) - бұл қосымша деңгей хаттамасы. Компьютерлер, ноутбуктер және мобильді құрылғылар жағдайында қосымша деңгей ролін әдетте браузер атқарады. IoT құрылғылары жағдайында қосымшалар деңгейі іске қосылған операциялық жүйе арқылы (егер ол ендірілген ОЖ жұмыс істеп тұрса) немесе микробағдарлама арқылы жүзеге асырылуы мүмкін.

MQTT соңғы жылдары IoT үшін жеңіл құрылымы мен пайдаланудың қарапайымдылығына байланысты IoT сахнасына шықты. MQTT хаттамасы Facebook Messenger-де қолданылуына және оның IoT-ке тікелей сілтемелеріне байланысты көпшіліктің назарында ілікті (Bryce т.б., 2018). 2011 жылы Люси Чжан және оның командасы Facebook-ке қосылып, Facebook мессенджерін әзірлей бастады. MQTT көмегімен олар дербес жұмыс істеу уақытын төмендетпей, Facebook серверлерімен тұрақты байланыс орната алды.

Қауіпсіздік – заттар интернеті қосымшаларын дайындаудың ажырамас бөлігі. Мұнда негізгі мақсат қарапайым күнделікті заттарды Интернетке қосу ғана емес, сонымен қатар әртүрлі соңғы нүктелер арасында деректерді қауіпсіз тасымалдау болып табылады. Осылайша интеллектуалды заттар интернеті қосымшалары әртүрлі талаптарды қанағаттандыруда тиімді және табысты болып қана қоймай, сонымен қатар жоғары сенімділікке ие болуы керек, яғни соңғы пайда-

ланушылардың құпиялылығын сақтау кез келген веб-қызметтің міндеті болып табылады.

Бізге MQTT қосымша деңгей хаттамасын пайдалана отырып, практикалық IoT әзірлеуге көшкен кезде, хаттамалар стегінде қол жетімді қауіпсіздік функцияларын түсіну маңызды. Бұл қауіпсіздік функцияларын IOT қосымшаларын әзірлеудің басынан бастап қолдану қажет. MQTT – шектеулі ресурстары бар IoT құрылғыларын қолдануына және желінің шектеулі өткізу қабілеттілігі кезінде деректер алмасуға арналған жеңілдетілген хаттама. IoT қосымшаларының масштабтылығының салдарынан құрылғылардың және жүйелердің осалдығын, сондай-ақ, олардың интернетте үнемі қол жетімділігін ескере отырып, MQTT хаттамасында желі деңгейінде, тасымалдау деңгейінде, сондай-ақ қосымша деңгейінде қосылған қауіпсіздік мүмкіндіктері бар. OSI деңгейлерінде әртүрлі қауіпсіздік мүмкіндіктерін қосу арқылы әртүрлі шабуыл түрлерін болдырмауға болады. Осы қауіпсіздік мүмкіндіктерінің барлығы әртүрлі жеткізушілер мен стандартты ұйымдар мойындаған стандартты механизмдер.

Бұл мақалада біз MQTT хаттамасының қауіпсіздік механизмдерін зерттейміз. Осы зерттеудің нәтижесі одан әрі MQTT хаттамасының негізіндезаттаринтернеті(IoT)үшінжаңа,жеңілдетілгенаутентификация механизмін жүзеге асыру барысында қажет болады. Зерттеу барысында MQTT хаттамасы арқылы екі IoT құрылғысы (Raspberry pi) арасында деректер алмасу жүзеге асырылды. Құрылғылардың бірі MQTT брокері және жазылушы-клиент, екіншісі жариялаушы-клиент рөлін атқарады. Брокер мен клиент арасында ақпарат алмасу үш түрлі тәсілмен жүзеге асырылды:

1. Ашық порт арқылы, яғни қорғаусыз қосылу. Бұл әзірлеу және практикалық қолданыстан бұрын MQTT-құрылғыларын сынау кезінде қолайлы. Брокер мен клиент арасында деректер шифрлаусыз қарапайым мәтін түрінде берілді.

2. Пайдаланушының аты мен құпия сөзін пайдалану арқылы қосылу. Бұл әдіс арқылы брокер клиенттің жеке басын тексере алады. Дегенмен, жіберу кезінде деректер шифрланбайды.

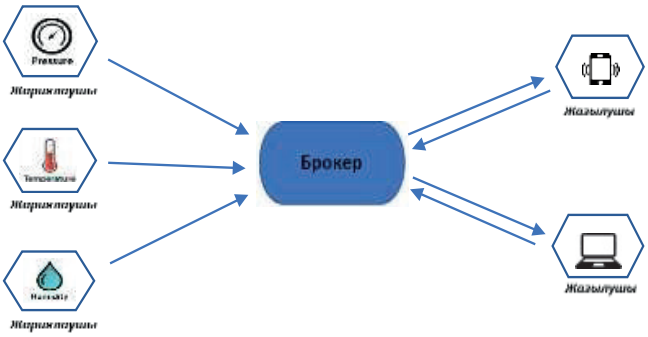
3. SSL шифрлауын пайдалану арқылы қосылу. Бұл Mosquitto MQTT брокерінде қол жетімді ең жетілдірілген шифрлау және аутентификациялау схемасы. SSL пайдалану кезінде сенімді сертификаттау орталығынан (Certificate Authority, CA) сервер сертификатын алу керек. Тестілеу үшін көбінесе өзбетімен жасалған сертификат дайындалады, оны сервер сертификатына қол қою үшін пайдалануға болады.

Зерттеу барысында Mosquitto MQTT брокері, Paho MQTT клиенті, OpenSSL утилитасы, iPerf құралы қолданылды.

Материалдар мен әдістер. 1.MQTT хаттамасы. MQTT (ағылш. message queuing telemetry transport) - TCP/IP үстінен жұмыс істейтін, жариялаушы-жазылушы принципі бойынша құрылғылар арасында хабарламалар алмасуға бағытталған жеңілдетілген желілік хаттама. MQTT немесе телеметрия хабарламалары кезегін тасымалдау хаттамасын 1999 жылы Энди Стэнфорд-Кларк (IBM) және Арлен Ниппер (Arcom, қазіргі Eurotech) ойлап тапты. 15 жылдан соң, яғни, 2014 жылы OASIS консорциумы MQTT 3.1.1 нұсқасын стандарттады және ол қазір ашық ISO (ISO / IEC 20922: 2016) стандарты болып табылады (Cornel – Cristian т.б., 2019). Бұл хаттама ең алғашқы рет мұнай құбырларын спутниктік қосылыстар арқылы қосу үшін дайындалды және оның жобалық параметрлері батареяны минималды шығындауды және өткізу жолағын минималды пайдалануды қамтыды (Katsikeas т.б., 2017) MQTT хаттамасының үстеме шығындары төмен, яғни ол қосымша деректердің аз көлемі мен нақты хабарлама мазмұнын ғана жібереді. MQTT тақырыпшасы HTTP немесе CoAP (Azzawi т.б., 2016.) сияқты басқа хаттамалармен салыстырғанда өте кішкентай (небәрі 2 байт) (Yassein т.б., 2017).

MQTT жариялау/жазылу архитектурасын қолдайды. MQTT хаттамасында екі клиент бар, бірі – жариялаушы (Publisher), екіншісі – жазылушы (Subscriber). Жариялаушы-клиент хабарламаны немесе пайдалы жүктемені (Payload) белгілі бір тақырыпта (Topic) жариялайды, ал жазылушы-клиент нақты тақырыпқа жазылып, хабарламаны алады да, сәйкес әрекеттерді орындайды. Тақырыптар – деректер тасымалданатын жолды анықтау үшін пайдаланылатын виртуалды арналар. Тақырыптың максималды ұзындығы MQTT сипаттамаларына сәйкес 65535 байтқа дейін болуы мүмкін. Тақырыптарды жариялаушылар жасайды және брокерге хабарламамен бірге жіберіледі, содан кейін жазылушы сол тақырыптарға жазыла алады.

MQTT хаттамасы арқылы IoT құрылғылары брокермен байланыса алады. IOT құрылғысын жариялаушы ретінде де, жазылушы ретінде де немесе екеуі ретінде MQTT брокерімен баптауға болады. MQTT хабарламаға бағытталған хаттама, онда клиенттер деректерді белгілі бір тақырыппен хабарлама ретінде жібереді және қабылдайды. 2-суретте MQTT хаттамасы арқылы «жариялау-жазылу» байланыс үлгісі көрсетілген. Бұл үлгіде брокер байланысудың орталық нүктесі болып табылады және ол арқылы клиенттер хабарламалармен алмасады.



2-сурет. Жариялау/жазылу байланыс үлгісі

Жариялаушы хабарламаларды жариялайды, ал жазылушы өзіне қатысты белгілі бір тақырыптарға жазылады және сол тақырыптар бойынша жарияланған әрбір хабарламаны алып отырады. Жарияланған хабарда брокер үшін бағыттау ақпаратын қамтитын тақырып бар. Әрбір хабарламаның тақырыбы бар және клиенттер бірнеше тақырыптарға жазыла алады. Брокер тақырыптарды орналастырады және жазылушыларға хабарламаларды қайта жіберуге жауапты. Белгілі бір тақырыпқа қатысты хабарларды алуға мүдделі кез келген клиент сол тақырыпқа жазылуы керек. Бұл тақырыптар компьютердегі файл жолдарына ұқсас иерархиялық жүйеде категорияларға бөлінген, мысалы, «Пәтер/қонақ_бөлме/кондиционер/күй» (Triawan т.б., 2016).

Пайдалы жүктеме – жариялаушы-клиент жібергісі келетін нақты хабарлама болып табылады. MQTT хаттамасы арқылы жіберуге болатын максималды пайдалы жүктеме 268, 435, 456 байтпен шектелген, бұл пакетке ең көбі 256 МБ болуы мүмкін. Ең үлкен өлшем MQTT спецификацияларымен шектелген.

Құрылғылар MQTT брокермен байланысу үшін белгілі бір хабарлама типтерін пайдаланады. Брокерден жіберілетін және алынатын хабарламалардың 14 типі бар. Негізгі хабарламаларға клиенттерді брокерге қосатын CONNECT/CONNACK, клиентке тақырыпқа жазылуға мүмкіндік беретін SUBSCRIBE/SUBACK және тақырып деректерін жариялаушыдан брокерге немесе брокерден жазылушыға жіберуге мүмкіндік беретін PUBLISH/PUBACK кіреді.

Әртүрлі IoT хаттамаларының арасында MQTT хаттамасының қызмет көрсету сапасы (QoS) оны бірегей етеді, және де хабарлардың жеткізілуі мен екі тарап арасында деректердің таралуына кепілдік береді (Kenzhebayeva т.б., 2021). MQTT хаттамасы байланыс үшін қызмет көрсету сапасының 3 түрін пайдаланады. MQTT қызмет көрсету

сапасы жариялаушы мен жазылушы арасында мәліметтердің түсуін растау туралы түсініктікті қамтамасыз етеді.

– QoS 0 – хабарлама бір рет ғана жіберіледі. Егер жеткізу үзілсе, онда хабарлама жоғалуы мүмкін – қайта жіберу болмайды.

– QoS 1 – хабарлама кемінде бір рет жіберіледі және алушы жеткізілгенін растайды. Бұл жағдайда хабарламаларды жіберу қайталануы мүмкін.

– QoS 2 – хабарлама мәселелер мен кедергілерге қарамастан хабарлама бір рет жеткізіледі. Сәтсіздікке байланысты жеткізу кешіктірілуі мүмкін, бірақ хабарлама бәрібір адресатқа жеткізіледі, мысалы, байланыс қалпына келтірілгеннен кейін.

2. MQTT хаттамасындағы қауіпсіздік механизмдері. MQTT мақсаты – Заттар интернеті үшін қолдануға жеңіл әрі қарапайым байланыс хаттамасын ұсыну. Хаттаманың өзінде тек бірнеше қауіпсіздік механизмдері анықталған. MQTT хаттамасында желі, транспорттық және қосымша деңгейлерінде қосылған қауіпсіздік функциялары бар. Әрбір деңгей әртүрлі шабуылдардан қорғайды.

Желілік деңгейде хаттама IoT құрылғыларын шлюз арқылы қосуды, содан кейін шлюзді VPN арқылы брокерге қосуды ұсынады. Құрылғылар Wi-Fi, Zigbee, Bluetooth және т.б. сияқты қауіпсіз физикалық деңгей хаттамалары арқылы шлюзге қосылуы керек.

Транспорттық деңгейде хаттама TLS/SSL қолданады. MQTT спецификациясында көрсетілгендей, TLS/SSL – стандартты транспорттық деңгей хаттамасы болып табылады, ол пакеттерді шифрлауға мүмкіндік береді, сонымен қатар сәйкесінше клиент пен сервер сертификаттарын пайдаланып клиент пен сервердің аутентификациясын қамтамасыз етеді.

Қолданба деңгейінде MQTT хаттамасы клиенттің аутентификациясы мен деректерді шифрлауды қамтамасыз етеді. Клиентті аутентификациялау әдетте брокер жағында клиент идентификаторы және пайдаланушы аты/құпия сөзі сияқты тіркелгі деректерінің көмегімен орындалады. MQTT хаттамасын қолдану кезінде транспорттық деңгейдегі толық шифрлауды немесе жай ғана пайдалы жүктемені шифрлауды орындауға болады.

MQTT спецификациясына сәйкес, MQTT хаттамасында келесі қауіпсіздік функциялары қарастырылған:

1) Аутентификация – бұл құрылғылар брокерге қосылып, басқа құрылғылармен әрекеттескенде түпнұсқалығын тексеру процесі. MQTT аутентификациясы пайдаланушы аты мен құпия сөз арқылы жүзеге асырылады. Аутентификацияға келгенде, MQTT хаттаманың

өзі CONNECT хабарында пайдаланушы аты мен құпия сөзі өрістерін береді. Сондықтан MQTT брокеріне қосылу кезінде клиентке пайдаланушы аты мен құпия сөзін жіберу мүмкіндігі болады. Клиентте пайдаланушы аты мен құпия сөзді орнатқаннан кейін олар брокерге мәтіндік форматта жіберіледі. Бұл шабуылдаушыға тыңдауға мүмкіндік береді. Осылайша, пайдаланушы аты мен құпия сөздің толық қауіпсіз берілуіне кепілдік берудің жалғыз жолы транспорттық шифрлауды пайдалану болып табылады.

Хаттама әрбір клиентке бірегей клиент идентификаторын беру арқылы кеңейтілген аутентификацияны қамтамасыз етеді. Бірегей клиент идентификаторын клиент MQTT CONNECT хабарламасында пайдаланады. Бірегей клиент идентификаторы ретінде 36 таңбадан тұратын UID кодын немесе желілік модульдің MAC мекен-жайы немесе құрылғының сериялық номері сияқты кез келген басқа бірегей ақпаратты пайдалануға болады.

2) Авторизация – ресурстарға қол жеткізу құқықтарын көрсету функциясы. Брокерге қосылғаннан кейін MQTT клиенті екі түрлі әрекет жасай алады: хабарламаларды жариялау және тақырыптарға жазылу. Клиентке ол рұқсат етілген тақырыптарды ғана жариялауға немесе жазылуға рұқсат беру үшін брокер жағында тақырыпқа рұқсат беруді жүзеге асыру қажет. Бұл рұқсаттар брокердің орындалуы кезінде конфигурацияланатын және реттелетін болуы керек. Тақырыпқа рұқсат берілу келесідей болуы мүмкін:

− Рұқсат етілген тақырып (нақты тақырып немесе қойылмалы таңбаларымен тақырып)

− Рұқсат етілген операциялар (жариялау, жазылу, екеуі де)

− Мүмкін қызмет көрсету деңгейі (0, 1, 2, барлығы)

Тақырыпқа рұқсат берудің бұл типі брокерге клиенттер үшін авторизация саясаттарын көрсетуге және олардың тақырыптарға жазылу және хабарларды жариялау мүмкіндігін шектеуге мүмкіндік береді.

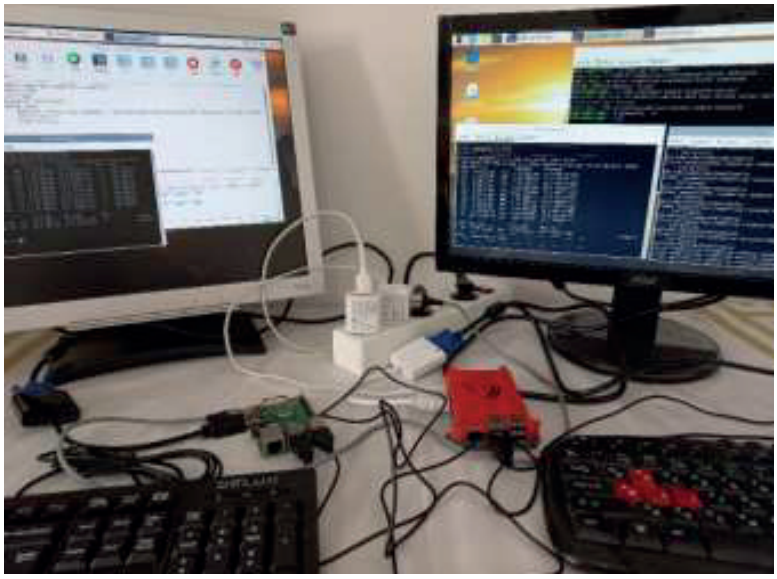
3) TLS/SSL қауіпсіздігі. MQTT хаттамасы үнсіз келісім бойынша шифрланған байланысты пайдаланбайтын TCP тасымалдау хаттамасына сүйенеді. Шифрлау мәселесін шешу үшін көптеген брокерлер қарапайым TCP орнына TLS пайдаланады, яғни TLS тасымалдау деңгейінде қауіпсіздікті қамтамасыз етеді. TLS көмегімен деректер пакеттерін шифрлау арқылы олардың мазмұнын үшінші тараптар оқуы немесе өзгертуі мүмкін емес. Қауіпсіз TLS/SSL MQTT байланысы үшін 8883 порты стандартталған. Көптеген брокерлер (мысалы, Mosquitto) TLS қауіпсіздігін қолдайды. MQTT TLS қауіпсіздік жүйесінде әрбір пакет шифрланатындықтан, бұл байланыс немесе қол алысудың

үстеме шығындарын арттырады. Ал шектеулі IoT құрылғылары үшін бұл мүмкін емес (Heer т.б., 2011). Әрине, егер IOT құрылғылары байланысқа кететін үстеме шығындарды көтере алатын болса, TLS әрқашан қолданылуы керек. Әзірлеушілер тасымалдау деңгейін толық шифрлау үшін TLS пайдаланады.

4) Пайдалы жүктемені шифрлау. MQTT хаттамасында пайдалы жүктемені шифрлау қосымша деңгейіндегі қауіпсіздікті қамтамасыз етеді. Әзірлеуші TLS қауіпсіздігін қолданбаған кезде, дегенмен, деректерді кәдімгі мәтін түрінде жібергісі келмесе, пайдалы жүктемені шифрлауды қолданады. Бұл қосымша қауіпсіздік деңгейін қамтамасыз етеді, себебі осылайша қосымшаның барлық деректері қорғалады және шифрланады. Пайдалы жүктемені шифрлау тасымалдау деңгейінде толық шифрлаудың орнына қосымшаның нақты деректерін шифрлауға мүмкіндік береді. Қосымшаның метадеректері (тақырып) шифрланбаған күйінде қалады. MQTT хаттамасында пайдалы жүктемені шифрлау кезінде PUBLISH пакеттерінің бөлігі ретінде пайдалы жүктемені шифрлауға болады. Пайдалы жүктеме әрқашан жариялаушы жағында шифрланады, ал дешифрлау процесі үздіксіз шифрлау жағдайында жазылушыда орындалуы мүмкін, бірақ оны брокерде де жасауға болады. Кез келген баптау барысында асимметриялық немесе симметриялық шифрлау схемаларын орнатуға болады. Сонымен қатар, кез келген сценарийде тек пайдалы жүктеме деректері шифрланады, ал барлық басқа деректер (клиент ақпараты, сертификаттар, тақырып туралы ақпарат) шифрланбаған күйде қалады. Қандай шифрлау/дешифрлау схемасы қолданылатынына байланысты, схеманың өзі көлемді ресурстарды қажет етеді, сондықтан бұл қайтадан шектеулі IoT құрылғылары үшін мәселе тудыруы мүмкін. Сондай-ақ барлық MQTT клиенттеріне кілттерді қауіпсіз жеткізу қажет болады. Жалпы, бұл шешімдер ортадағы адам шабуылдарына немесе қайталап ойнату шабуылдарының жолын кеспейді.

3. IoT құрылғылары арасында ақпарат алмасуды жүзеге асыру. IoT құрылғылары ретінде Raspberry Pi 3 model B микрокомпьютерлері қолданылды. Олар келесі сипаттамаларға ие: CPU (орталық процессор) – ARM Cortex-A53, процессор жиілігі - 1,2 ГГц, RAM (оперативті жады) – 1 ГБ.

Олардың бірі брокер және жазылушы ретінде, екіншісі жариялаушы ретінде бапталды. 4-суретте IoT құрылғылары арасында ақпарат алмасу процесі көрсетілген.



3-сурет. IoT құрылғылары арасында ақпарат алмасу процесі

Брокер ретіндегі Raspberry Pi 3 model B микрокомпьютеріне MQTT брокері Eclipse Mosquitto орнатылды. Mosquitto ресми веб-сайтындағы мәліметтерге сәйкес, Eclipse Mosquitto – Mosquito MQTT хаттамасын жүзеге асыратын, ашық бастапқы коды бар хабарлама брокері, жеңіл және қуаттылығы төмен бір тақталы компьютерлерден бастап толық серверлерге дейін барлық құрылғыларда пайдалануға жарамды.

Біз Mosquitto MQTT брокерін үш түрлі баптадық:

Бірінші қадамда қосылымды тексеру үшін қарапайым MQTT болды. Қарапайым MQTT-де шифрлау да немесе аутентификациялау да жоқ. Брокерді таба алатын кез келген нысан оған қосылып, оны қадағалай алады немесе оған хабарламалар жібере алады. Бұл қосылу негізгі MQTT қызметінің жұмыс істеп тұрғанын тексеру үшін уақытша, алдын ала орындалатын қадам болуы керек.

Екіншісі қадам логинді қажет ететін қарапайым, бірақ шифрланбаған аутентификация болды. MQTT қосылу кезінде пайдаланушы аты мен құпия сөзді талап ететіндей бапталды.

Үшінші қадам TLS шифрлауын және негізгі аутентификацияны қосу болды. TLS тек брокер үшін ғана емес, әрбір клиент үшін x509 сертификаттарын талап етеді, өйткені MQTT өзара аутентификацияны қажет етеді. Яғни, клиент серверге аутентификация жасайды, ал сервер клиентке аутентификация жасайды. Бұл қадамда жай ғана бөліктерді жеке сынауға болмайды және әрбір бөлік бір-біріне сәйкес келуі және

тұтас жұмыс істеуі үшін дұрыс болуы керек. X.509 сертификаты - бұл пайдаланушы немесе құрылғы туралы ақпаратты және олардың сәйкес ашық кілтін қамтитын стандартты өрістер жиынтығы. X.509 стандарты сертификатқа қандай ақпарат кіретінін және оның кодталуын (деректер пішімі) анықтайды (Forsby т.б., 2018).

Осы үш қадам бойынша бапталған MQTT брокері мен екінші IoT құрылғысы (жариялаушы-клиент) арасында ақпарат алмасуды орындадық және сәйкесінше әрбір қадам бойынша желінің өткізу қабілеті өлшенді. 4-суретте желінің өткізу қабілетін өлшеу процесінен үзінді көрсетілген.

```
Connecting to host 192.168.43.200, port 5201
[  5] local 192.168.43.89 port 46338 connected to 192.168.43.200 port 5201
[ ID] Interval           Transfer     Bitrate         Retr  Cwnd
[  5]   0.00-1.00   sec  1.70 MBytes  14.2 Mbits/sec    0    129 KBytes
[  5]   1.00-2.00   sec  1.80 MBytes  15.1 Mbits/sec    0    212 KBytes
[  5]   2.00-3.00   sec  1.74 MBytes  14.6 Mbits/sec    0    283 KBytes
[  5]   3.00-4.00   sec  1.43 MBytes  12.0 Mbits/sec    0    358 KBytes
[  5]   4.00-5.00   sec  1.68 MBytes  14.1 Mbits/sec    0    437 KBytes
[  5]   5.00-6.00   sec  1.49 MBytes  12.5 Mbits/sec    1    430 KBytes
[  5]   6.00-7.00   sec  1.43 MBytes  12.0 Mbits/sec   26    380 KBytes
```

4-сурет. Желінің өткізу қабілетін өлшеу процесінен үзінді

Желінің өткізу қабілетін өлшеу Iperf утилитасының көмегімен жүзеге асырылды. Iperf – желі қосылымының өнімділігін және екі құрылғы арасындағы деректерді берудің максималды жылдамдығын өлшеуге көмектесетін қарапайым және ыңғайлы желілік утилита.

Нәтижелер. Алдыңғы бөлімде IoT құрылғылары арасында ақпарат алмасуды жүзеге асырудың үш түрлі қадамын сипаттаған болатынбыз. Әр қадамға толығырақ тоқталып өтейік.

Бірінші қадам бойынша MQTT брокеріне клиент қарапайым қосылу жүзеге асырылды. Ол үшін Mosquito MQTT брокері іске қосылған соң жазылушы-клиент нақты тақырыпқа жазылды. Бірақ осы тақырып бойынша жариялаушы-клиент хабарлама жарияламайынша жазылушы-клиент күту күйінде болады. mosquitto_sub және mosquitto_pub командалары сәйкесінше тақырыпқа жазылуды және жариялауды жүзеге асырады. Бірінші қадам барысында 30 байт пайдалы жүктеме әрбір 3 секунд сайын жариялаушы-клиенттен брокерге жөнелтілді, және жазылушы-клиент терминалында көрініс тапты. Iperf құралымен 10 секунд бойы (үнсіз келісім бойынша) өлшеу 50 рет орындалды. Нәтижесінде орта есеппен желінің өткізу қабілеті - 13,4 мбит/с құрады.

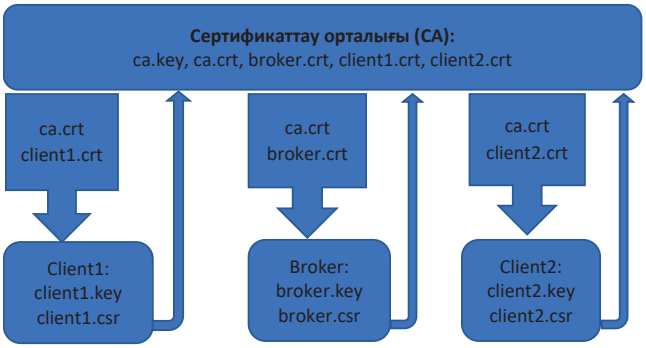
Екінші қадам бойынша MQTT брокеріне пайдаланушы аты мен

құпия сөзді талап ететін аутентификацияны орындау арқылы қосылу жүзеге асырылды. Жалпы жұмыс істеп тұрған MQTT брокеріне сервердің IP-адресін білетін кез-келген нысан қосыла алады. Бұл қауіпсіздік мәселесін шешу үшін хабарлама жіберуге рұқсат алған пайдаланушылардың аты мен құпия сөздерін көрсету керек. Mosquitto брокері қосылатын пайдаланушылар үшін құпия сөздерді шифрлау құралын қосады. sudo mosquitto_passwd -c /etc/mosquitto/passwd User1 командасы User1 пайдаланушыны қосады, осыдан соң екі рет құпия сөз енгізу ұсынылады. Пайдаланушыларды және олардың құпия сөздерін енгізген соң, Mosquitto брокерінің конфигурация файлына allow_ anonymous false және password_file /etc/mosquitto/passwd жолдарын енгізу керек. Осыдан кейін жариялаушы-клиент те, жазылушы-клиент те жүйеге ену үшін пайдаланушы атауы мен құпия сөзді енгізуі қажет болады. Екінші қадам барысында да 30 байт пайдалы жүктеме әрбір 3 секунд сайын жариялаушы-клиенттен брокерге жөнелтілді, және жазылушы-клиент терминалында көрініс тапты. Iperf құралымен 10 секунд бойы өлшеу жүргізілді. Бұл сынама да 50 рет орындалды. Нәтижесінде орта есеппен желінің өткізу қабілеті - 10,4 мбит/с құрады.

Үшінші қадам бойынша mosquitto MQTT брокерін TLS қауіпсіздігін қолдану үшін баптадық.

Біз openssl қосымшасын жеке сертификаттау орталығын (CA), сервер кілттері мен сертификаттарды жасау үшін қолдандық. 5-суретте Openssl құралымен сертификаттарды дайындау схемасы көрсетілген. Ең алдымен сертификаттау орталығының кілті (ca.key) дайындалады және осы кілт арқылы сертификаттау орталығының сертификаты (ca. crt) дайындалады. Сертификаттау орталығының кілті (ca.key) құпия сөзбен қорғалады. Осыдан соң брокердің және клиенттердің кілттері (broker.key, client1.key, client2.key) жеке-жеке дайындалады да, осы кілттердің негізінде сертификаттау орталығынан сертификаттар дайындауға сұраныстар (broker.csr, client1.csr, client2.csr) жеке-жеке дайындалып, сертификаттау орталығына жөнелтіледі. Сертификаттау орталығы осы сұраныстар (broker.csr, client1.csr, client2.csr) және өзінің кілті (ca.key) негізінде брокер мен клиенттерге сертификаттар (broker. crt, client1.crt, client2.crt) дайындап, жібереді. Әрбір сертификатпен қосып, сертификаттау орталығының сертификаты да (ca.crt) брокер мен клиенттердің қоймаларында сақталуы тиіс. Осылайша openssl құралының көмегімен біз TLS/SSL қосылысына қажетті сертификаттар жиынтығын дайындап, брокер мен әрбір клиенттердің қоймаларына орналастырдық.

5-сурет. Openssl құралымен сертификаттарды дайындау.



Осыдан кейін Mosquitto брокерінің конфигурация файлына қажетті ақпараттарды енгіземіз, яғни сертификаттардың орналасуы, порттар, сертификаттарды сұрау параметрлерін орнатамыз. Брокерді жұмысқа дайындаған соң mosquitto_sub және mosquitto_pub командалары арқылы, сертификаттардың орналасуын көрсете отырып, сәйкесінше тақырыпқа жазылуды және жариялауды жүзеге асырадық. Үшінші қадам барысында да 30 байт пайдалы жүктеме әрбір 3 секунд сайын жариялаушы-клиенттен брокерге жөнелтілді, және жазылушы-клиент терминалында көрініс тапты. Iperf құралымен 10 секунд бойы өлшеу 50 рет орындалды. Нәтижесінде орта есеппен желінің өткізу қабілеті - 8,48 мбит/с құрады.

Талқылау. Сынақтамада екі IoT құрылғысы (Raspberry Pi 3 model B микрокомпьютерлеі) арасында MQTT хаттамасы арқылы ақпарат алмасу процесі қауіпсіздік тұрғысынан зерттелді. Олардың бірі брокер және жазылушы-клиент ретінде, екіншісі жариялаушы-клиент ретінде бапталды. MQTT брокері ретінде Eclipse Mosquitto (https://mosquitto.org/download/) орнатылды. MQTT клиенті Mosquitto серверіне үш жолмен қосылды:

– қорғалмаған арна арқылы;

– пайдаланушы аты және құпия сөзді қолданумен қорғалған арна арқылы;

– TLS хаттамасымен қорғалған арна арқылы;

Сынақтамада өлшенген осы үш арнаның өткізу қабілеті 1-кестеде және 6-суретте көрсетілгендей болды.

1-кесте. Арналардың өткізу қабілеті

№	Арналар	Өткізу қабілеті, мбит/с
1	қорғалмаған арна арқылы;	13,4

2	пайдаланушы аты және құпия сөзді қолданумен қорғалған арна арқылы;	10,4
3	TLS хаттамасымен қорғалған арна арқылы;	8,48

6-сурет. Арналардың өткізу қабілеті.

Сынақтама жоғарыда айтылған қосылымдардың әрқайсысынан 50 рет орындалды. Нәтижесінде TLS хаттамасымен қорғалған арна арқылы қосылу желінің өткізу қабілетін едәуір азайтатыны көрінді. Демек IoT құрылғылары үшін жаңа жеңілдетілген аутентификация схемасы қажет.

Қорытынды. Соңғы кездері MQTT хаттамасының IoT қосымшалары үшін қолайлы, ең жақсы нұсқа болып табылатындығы белгілі болды. Сондықтан, MQTT хаттамасын қолданып IoT қосымшалары үшін жақсы шешімдер алу мақсатында көптеген зерттеулер жүргізілуде (Soni т.б., 2017). Осы зерттеулердің бір бағыты MQTT хаттамасының негізінде орындалған қосымшалар үшін жүзеге асырылуы тиіс қауіпсіздік шаралары. Ал MQTT хаттамасында тиімді қауіпсіздік функциялары жетіспейді, сондықтан тасымалдау деңгейнде SSL/TLS қолданылады. TLS жақсы қауіпсіз нұсқа болғанымен, үшінші тарапты жұмылдыру, сертификаттарды энергияға тәуелсіз жадыда сақтау және т.б. ресурсы шектеулі IoT құрылғылары үшін қосымша талаптар қояды. Сондықтан біздің мақсатымыз - болашақта MQTT хаттамасына негізделген заттар интернеті (IoT) үшін жаңа жеңілдетілген аутентификация механизмін ұсыну. Осы мақалада MQTT хаттамасының қауіпсіздік механизмдері зерттелді. MQTT хаттамасының спецификациясына сәйкес онда қарастырылған қауіпсіздік шаралары IoT құрылғысында (Raspberry pi) жүзеге асырылды және нәтижесі өлшенді. Сынақтама нәтижесінде қорғалмаған арна арқылы ақпарат алмасумен салыстырғанда пайдаланушы аты және құпия сөзді қолданумен қорғалған арна арқылы және TLS хаттамасымен қорғалған арна арқылы ақпарат алмасу кезінде

арнаның өткізу қабілетіне айтарлықтай әсер ететіні белгілі болды. Осы зерттеудің нәтижесі біздің алдағы зерттеулерде пайдалы болады деп есептейміз.

Information about authors:

Kazhenova Zhanar – Doctoral Student, Department of Computing and Software, S. Seifullin Kazakh Agrotechnical University, Nur-Sultan, Kazakhstan; zhkazhenova75@gmail.com; ORCID ID: https://orcid.org/0000-0001-9022-7169;

Kenzhebayeva Zhanat – Candidate of technical sciences, acting associate professor, Department of Computing and Software, S. Seifullin Kazakh Agrotechnical University, Nur-Sultan, Kazakhstan; kenzhebayeva.zh@gmail.com; ORCID ID: https://orcid.org/0000-0002-1942-4474;

Aleksander Prudnik – Candidate of technical sciences, Associate Professor, Department of Engineering Psychology and Ergonomics, Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus; aleksander.prudnik@bsuir.by; ORCID ID: *https://orcid.org/0000-0002-6180-1819*.

ӘДЕБИЕТТЕР

Andy S., Rahardjo B. and Hanindhito B., “Attack scenarios and security analysis of MQTT communication protocol in IoT system,” 2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), Yogyakarta, 2017, pp. 1-6.

Azzawi MA., Hassan R., Bakar KAA., “A Review on Internet of Things (IoT) in Healthcare” International Journal of Applied Engineering Research, November 2016.

Bryce R., Srivastava G.: The addition of geolocation to sensor networks. In: ICSOFT. pp. 796–802. SciTePress (2018).

Cornel-Cristian A., Gabriel T., Arhip-Calin M., Zamfirescu A., “Smart home automation with MQTT” 54th International Universities Power Engineering Conference (UPEC), 2019.

Filip Forsby et al. “Lightweight X.509 Digital Certificates for the Internet of Things”. In: (2018). Ed. by Giancarlo Fortino et al., pp. 123–133.

Goyal K.K., Garg A., Rastogi A., Singhal S., “A Literature Survey on Internet of Things (IoT),” Int. J. Advanced Networking and Applications. Volume: 09 Issue: 06 Pages: 3663-3668, 2018.

Heer T., Garcia-Morchon, O., Hummen, R., Keoh, S.L., Kumar, S.S., Wehrle, K.: Security challenges in the ip-based internet of things. Wireless Personal Communications 61(3), 527–542 (2011).

Каженова Ж.С., Кенжебаева Ж.Е. Безопасность в протоколах и технологиях IoT: обзор. International Journal of Open Information Technologies ISSN: 2307-8162 vol. 10, no. 3, 2022.

Katsikeas S., Fysarakis K., Miaoudakis A., Van Bemten A., Askoxylakis I., Papaefstathiou I., Plemenos A., "Lightweight secure industrial iot communications via the mq telemetry transport protocol," in Computers and Communications (ISCC), 2017 IEEE Symposium on, pp. 1193–1200, IEEE, 2017.

Kenzhebayeva Z., Akhmetova Z., Bainazarova R., Kazhenova Z., Sariyeva A. Simplified and secure authentication scheme for the internet of things(article) Journal of Theoretical and Applied Information TechnologyVolume 99, Issue 24, 5 December 2021, Pages 5774-5782.

Soni D., Makwana A., "A Suever on Mqtt: A Protocol of Internet Of Things (IOT)" April 2017. Conference: International conference on telecommunication, power analysis and computing techniques (ICTPACT - 2017).

Triawan M.A., Hindersah H., Yolanda D., Hadiatna F. "Internet of things using publish and subscribe method cloud-based application to NFT-based hydroponic system" 6th International Conference on System Engineering and Technology (ICSET, 2016.

Yassein M.B., Shatnawi M.Q., Aljwarneh S., Al-Hatmi R., "Internet of Things: Survey and open issues of MQTT protocol" International Conference on Engineering & MIS (ICEMIS), 2017.

REFERENCES

Andy S., Rahardjo B. and Hanindhito B., "Attack scenarios and security analysis of MQTT communication protocol in IoT system," 2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), Yogyakarta, 2017, pp. 1-6.

Azzawi M.A., Hassan R., Bakar K.A.A., "A Review on Internet of Things (IoT) in Healthcare" International Journal of Applied Engineering Research, November 2016.

Bryce R., Srivastava G.: The addition of geolocation to sensor networks. In: ICSOFT. pp. 796 – 802. SciTePress (2018).

Cornel-Cristian A., Gabriel T., Arhip-Calin M., Zamfirescu A., "Smart home automation with MQTT" 54th International Universities Power Engineering Conference (UPEC), 2019.

Filip Forsby et al. "Lightweight X.509 Digital Certificates for the Internet of Things". In: (2018). Ed. by Giancarlo Fortino et al., pp. 123–133.

Goyal K.K., Garg A., Rastogi A., Singhal S., "A Literature Survey on Internet of Things (IoT)," Int. J. Advanced Networking and Applications. Volume: 09 Issue: 06 Pages: 3663-3668, 2018.

Heer T., Garcia-Morchon O., Hummen R., Keoh S.L., Kumar S.S., Wehrle K.: Security challenges in the ip-based internet of things. Wireless Personal Communications 61(3), 527–542 (2011).

Kazhenova Z.S., Kenzhebayeva Z.E., Security in IoT protocols and technologies: an overview. International Journal of Open Information Technologies ISSN: 2307-8162 vol. 10, no. 3, 2022.

Katsikeas S., Fysarakis K., Miaoudakis A., Van Bemten A., Askoxylakis I., Papaefstathiou I., Plemenos A., "Lightweight secure industrial iot communications via the mq telemetry transport protocol," in Computers and Communications (ISCC), 2017 IEEE Symposium on, pp. 1193–1200, IEEE, 2017.

Kenzhebayeva Z., Akhmetova Z., Bainazarova R., Kazhenova Z., Sariyeva A. Simplified and secure authentication scheme for the internet of things(article) Journal of Theoretical

and Applied Information TechnologyVolume 99, Issue 24, 5 December 2021, Pages 5774-5782.

Soni D., Makwana A., "A Suever on Mqtt: A Protocol of Internet Of Things (IOT)" April 2017. Conference: International conference on telecommunication, power analysis and computing techniques (ICTPACT - 2017).

Triawan M.A., Hindersah H., Yolanda D., Hadiatna F. "Internet of things using publish and subscribe method cloud-based application to NFT-based hydroponic system" 6th International Conference on System Engineering and Technology (ICSET, 2016.

Yassein M.B., Shatnawi M.Q., Aljwarneh S., Al-Hatmi R., "Internet of Things: Survey and open issues of MQTT protocol " International Conference on Engineering & MIS (ICEMIS), 2017.

МАЗМҰНЫ

СОДЕРЖАНИЕ

CONTENTS

Publication Ethics and Publication Malpracticein
the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethicalguidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any otherlanguage, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайтах:
www:nauka-nanrk.kz
http://physics-mathematics.kz/index.php/en/archive
ISSN2518-1726 (Online),
ISSN 1991-346X (Print)

Директор отдела издания научных журналов НАН РК *А. Ботанқызы*
Заместитель директор отдела издания научных журналов НАН РК *Р. Жәлиқызы*
Редакторы: *М.С. Ахметова, Д.С. Аленов*
Верстка на компьютере *Г.Д.Жадыранова*

Подписано в печать 15.09.2022.
Формат 60х881/8. Бумага офсетная. Печать – ризограф.
17,5 п.л. Тираж 300. Заказ 3.

Национальная академия наук РК
050010, Алматы, ул. Шевченко, 28, т. 272-13-19