НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

«До захисту допущено»
В.о. завідувача кафедри
_____
М.В.Грайворонський
(підпис)

“_____”_____2019р.

Дипломна робота

на здобуття ступеня бакалавра

з напряму підготовки 6.170101 «Безпека інформаційних і комунікаційних систем»
на тему: Автентифікація в мережах інтернету речей

Виконав (-ла): студент (-ка) 4 курсу, групи ФБ-52
(шифр групи)

Нестріляй Богдан Сергійович _____ _____
(прізвище, ім’я, по батькові) (підпис)

Керівник Коломицев Михайло Володимирович _____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____ _____
(назва розділу) (посада, вчене звання, науковий ступінь, прізвище, ініціали) (підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій дипломній роботі
немає запозичень з праць інших авторів
без відповідних посилань.
Студент _____
(підпис)

Київ - 2019 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)

Напрям підготовки 6.170101 «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ М.В.Грайворонський
(підпис)
«___»_____2019 р.

ЗАВДАННЯ
на дипломну роботу студенту

Нестріляй Богдан Сергійович _____
(прізвище, ім'я, по батькові)

1. Тема роботи Автентифікація в мережах інтернету речей _____
_____
_____,
науковий керівник роботи Коломицев Михайло Володимирович, к.т.н., доц. Каф. ІБ_____
_____
_,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «____ » 2019 р. № _____

2. Термін подання студентом роботи 10 червня 2019 р.

3. Вихідні дані до роботи _____
_____
_____
_

4. Зміст роботи _____

_____
_____
_____
_____

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо) _____
_____
_____
_____

6. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка

Студент _____ Нестріляй Б.С.
(підпис) (ініціали, прізвище)

Науковий керівник роботи _____ Коломицев М. В.
(підпис) (ініціали, прізвище)

РЕФЕРАТ

Робота обсягом 98 сторінок містить 7 ілюстрацій, 8 таблиць та 142 літературні посилання.

Метою роботи є створення математичного методу оцінки ефективності засобів автентифікації в мережах інтернету речей в залежності від заданих параметрів (важливість та кількість існуючих видів атак, наявність певних криптографічних механізмів); збір інформації про існуючі методи автнтифікації шляхом аналізу та метааналізу і застосування розробленого методу на ці дані. Результатом є ефективний та легко розширювальний спосіб вибору засобу автентифікації в залежності від потреб користувача

Об’єктом дослідження є засоби автентифікації в мережах інтернету речей.

Результати роботи викладені у вигляді таблиці та методу, що демонструє, ефективність обраних для аналізу методів автентифікації згідно запропонованого методу.

Результати роботи можуть бути використані при розробці систем інтернету речей. Також можна використовувати розроблений метод для оцінки ефективності методів автентифікації та порівняння з результатами оцінки інших методів автентифікації.

Автентифікація, інтернет речей, оцінка ефетивності, аналіз, метааналіз, модель загроз, протоколи автентифікації.

ABSTRACT

The work in 98 page volume contains 7 illustrations, 8 tables and 142 literary references.

The purpose of the work is to create a mathematical method for assessing the effectiveness of authentication tools in IoT networks, depending on the given parameters (importance and number of existing types of attacks, the presence of certain cryptographic mechanisms); collect information on existing methods of outsourcing by analyzing and meta-analysis and applying the developed method to these data. The result is an efficient and easy way to select an authentication tool depending on the user's needs

The object of research is the means of authentication in the Internet of things.

The results of the work are presented in the form of a table and method demonstrating the effectiveness of the selected methods for analyzing authentication methods according to the proposed method.

The results of the work can be used in the development of IoT systems. Also, it can be used to evaluate the effectiveness of authentication methods and compare them with the results of evaluating other authentication methods.

authentication, Internet of Things, appraisal evaluation, analysis, meta-analyst, a model of threats, authentication protocols.

ЗМІСТ

Перелік умовних позначень, символів, одиниць, скорочень та термінів……..……..…...8
Вступ……..……..…….10
1 Аналіз проблем безпеки інтернету речей..…….....11
1.1 Загрози та механізми безпеки Інтернету речей…….…….....11
1.2 Автентифікація Інтернету речей……..……...16
1.3 Постановка задачі……..……...22
Висновки до розділу 1……/…...…….23
2 Дослідження бази забезпечення безпеки в мережах інтернету речей..……..……...25
2.1 Моделі загроз в IoT……..…….25
2.2 Існуючі моделі автентифікації в IoT…….……..40
2.3 Аналіз конфіденційності в протоколах IPsec и TLS…….49
2.4 Автентифікація в протоколах IPsec……...59
Висновки до розділу 2……..……..……..67
3 Побудова методу оцінки ефективності засобів автентифікації…….....68
3.1 Підготовка моделі загроз……..…….…….68
3.2 Розробка методу оцінювання засобів автентифікації…..……71
3.3 Результати оцінки методів автентифікації в IoT…….…….....73
Висновки до розділу 3…….……...……..83
Висновки…….……..84
Перелік джерел посилань……...……....85

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ ТА ТЕРМІНІВ

Автентифікація - процедура встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора

Інтернет речей - концепція систем, що складається із взаємозв'язаних фізичних пристроїв, які мають вбудовані давачі, а також програмне забезпечення, що дозволяє здійснювати передачу і обмін даними між фізичним світом і комп'ютерними системами, за допомогою використання стандартних протоколів зв'язку. Окрім датчиків, мережа може мати виконавчі пристрої, вбудовані у фізичні об'єкти і пов'язані між собою через дротові чи бездротові мережі. Ці взаємопов'язані пристрої мають можливість зчитування та приведення в дію, функцію програмування та ідентифікації, а також дозволяють виключити необхідність участі людини, за рахунок використання інтелектуальних інтерфейсів

Модель загроз - абстрактний формалізований чи неформалізований опис методів і засобів здійснення загроз.

IPsec (скорочення від IP Security) — набір протоколів для забезпечення захисту даних, що передаються за допомогою протоколу IP, дозволяє здійснювати підтвердження справжньості та/або шифрування IP-пакетів

TLS - криптографічний протокол, що надає можливості безпечної передачі даних в Інтернет для навігації, отримання пошти, спілкування, обміну файлами, тощо на прикладному рівні.

Апаратний ідентифікатор - ідентифікатор, що присвоюється тому чи іншому пристрою на основі певного алгоритму або засобу (MAC, IPv4, IPv6)

MAC-адреса - це унікальний ідентифікатор мережевого інтерфейсу (зазвичай мережевої карти) для реалізації коммунікації пристроїв в мережі

на фізичному рівні. Це унікальний номер, який зберігається у пам'яті, що доступна тільки для читання, призначена мережевій карті її виробником.

IP-адреса - це ідентифікатор (унікальний числовий номер) мережевого рівня, який використовується для адресації комп'ютерів чи пристроїв у мережах, які побудовані з використанням протоколу TCP/IP.

Атака — детально підібраний набір дій, які, в разі успіху, призведуть або до пошкодження ресурсів веб-застосунку або до небажаної операції.

Радіочастотна ідентифікація (RFID) - це бездротова технологія, яка складається з тегів, які можуть бути прикріплені до будь-якого фізичного об'єкта або навіть до людей; його основною метою є виявлення або виявлення об'єктів з тегами.

Віртуальна приватна мережа (VPN) — узагальнююча назва мереж, що створюються поверх інших мереж, які мають менший рівень довіри.

ВСТУП

Актуальність роботи: IoT - одна з найпрогресивніших технологій нашого часу. Вона здатна полегшити та зберегти життя багатьом людям, але однією з основних проблем Інтернету Речей є безпека і через багато невирішених проблем в цій сфері IoT відштовхує від себе багатьох нових користувачів та сповільнює темпи росту даної технології.

Мета і завдання дослідження: Об’єктом дослідження даної роботи є автентифікація в мережах інтернету речей. Предметом дослідження є ефективність та надійність новітніх методів забезпечення безпеки в IoT. Головною метою даної роботи є метааналіз досліджень найпопулярніших та найефективніших засобів автентифікації в мережі речей, а також розробка математичної моделі оцінки протоколів в залежності від потреб користувача і його пріорітетів.

Методи дослідження: Під час виконання роботи для збору інформації про різні засоби автентифікації досліджувалися університетські публікації, статті в технічних журналах, спеціалізована література, семінари та форуми. Для побудови математичної моделі було проаналізовано існуючі ефективні способи оцінки протоколів автентифікації, що описані в спеціалізованій літературі.

Наукова новизна одержаних результатів: Враховуючи масштабність дослідження та гнучкість побудованої моделі, результатом роботи є інструмент, що дозволяє легко обрати потрібний в конкретній ситуації протокол автентифікації, а також легко розширювати даний механізм. Як приклад було обрано засіб автентифікації, що відповідає певним потребам.

1 **АНАЛІЗ ПРОБЛЕМ БЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ**

1.1 Загрози та механізми безпеки Інтернету речей

Спочатку дамо визначення основному об’єкту дослідження роботи, а саме IoT або ж інтернету речей. У самому широкому сенсі термін IoT охоплює все, що пов'язане з Інтернетом, але він все частіше використовується для визначення об'єктів, які «говорять» один з одним. Просто, Інтернет речей складається з пристроїв - від простих датчиків до смартфонів і носіїв - з'єднаних разом. Об'єднуючи ці підключені пристрої з автоматизованими системами, можна "збирати інформацію, аналізувати її і створювати дії", щоб допомогти людині з певним завданням або дізнатися з процесу. Насправді, це варіюється від розумних дзеркал до маяків у магазинах і за його межами.

У промисловому застосуванні датчики на виробничих лініях можуть підвищити ефективність і знизити кількість відходів. Одне дослідження показує, що 35% американських виробників вже використовують дані від інтелектуальних датчиків. Американські фірми Concrete Sensors створили пристрій, який можна вставити в бетон, наприклад, для надання даних про стан матеріалу.

Іншими словами, Інтернет Речей - це концепція підключення будь-якого пристрою (до тих пір, поки він має вимикач вкл / викл) до Інтернету та інших підключених пристроїв. IoT - це гігантська мережа пов'язаних речей і людей, які збирають і обмінюються даними про те, як вони використовуються, і про навколишнє середовище.

Це включає в себе надзвичайну кількість об'єктів будь-якої форми та розмірів - від розумних мікрохвильових печей, які автоматично готують вашу їжу на потрібний проміжок часу, до самостійних автомобілів, складні сенсори яких виявляють об'єкти на своєму шляху, до пристосованих приладів, що вимірюють частоту серцевих скорочень і кількість кроків, які

ви зробили в цей день, а потім скористайтеся цією інформацією, щоб запропонувати ваші плани навчання. Є навіть пов'язані футбольні м'ячі, які можуть відстежувати, як далеко і швидко вони кидаються, і записувати цю статистику через додаток для майбутніх навчальних цілей.

Серед головних переваг інтернету речей:

1. Безпека, комфорт, ефективність

Серед IoT рішень багато таких, що забезпечують набагато більший рівень комфорту (контрольовані кавоварки, пральні машинки і т.п.), безпеки (wi-fi камери, дистанційні сигналізації та різного роду детектори), а також засоби для збільшення ефективності праці. Також великим впливом IoT відзначився на небезпечних виробництвах, де за допомогою таких застосунків зменшують вплив шкідливих чинників на працівників, а також сприяють розвитку бізнесу

2. Краще прийняття рішень

Якщо ми можемо аналізувати більше тенденцій з емпіричних даних, то ми можемо приймати розумніші рішення. IoT надає доступність даних у кожному аспекті вашого бізнесу. Розглянемо цикли тестування. Вони радикально скорочуватимуться, знижуючи витрати на оптимізацію процесу. Крім того, видимість в поведінці системи може дати нові уявлення та ідеї. Це може керувати бізнесом, як ніколи раніше.

3. Генерація доходів

По-перше, перераховані вище переваги вплинуть на нижній прибуток підприємст, що будуть використовувати IoT, зменшуючи витрати. IoT також допоможе підвищити ефективність. Але, лише питання часу, перш ніж аналіз даних IoT допоможе вам реалізувати нові бізнес-функції. Також це призведе до нових можливостей отримання доходу. IoT може бути спеціальним «фактором X». Його унікальність надає багатьом організаціям стратегічну перевагу над конкурентами. Ця перевага буде корисною для компаній і в наступному десятилітті.

Але при всих перевагах інтернету речей йому присутні деякі проблеми, а саме:

1. Блокування Інтернету

Згідно з даними Всесвітнього економічного форуму, зростаюча кількість прикордонних атак почне підштовхувати національні уряди до руйнування Інтернету в національних або навіть регіональних «стінах». Існують і інші тиски, які підштовхнуть їх до цього, включаючи економічні. протекціонізм, регуляторні розбіжності та втрата державної влади щодо глобальних інтернет-компаній.

Це створить серйозні проблеми для концепції - і практики глобального IoT -, що призведе до створення бар'єрів для потоку контенту та транзакцій. Деякі могли б вітати перехід до менш гіпер-глобалізованого онлайн-світу, але багато хто не хотів би, опір буде, швидше за все, як і швидке зростання незаконних обхідних шляхів. Темпи розвитку технологій будуть сповільнюватися, і його траєкторія зміниться

2. Атаки на хмарні середовища

Враховуючи, що велика кількість даних, які будуть запускатися в IoT, зберігатиметься в хмарі, ймовірно, що провайдери хмари стануть однією з головних цілей у цій війні. Хоча зростає усвідомлення цієї проблеми, кібербезпека все ще недостатньо забезпечена ресурсами в порівнянні з потенційними масштабами загрози. Щоб отримати якусь ідею про проблему, доповідь Всесвітнього економічного форуму наводить аналіз, який свідчить про те, що видалення одного постачальника послуг у хмарі може призвести до економічного збитку в розмірі $ 50 мільярдів до $ 120 мільярдів

3. Проблеми, пов'язані зі створенням AI

Розроблені складні, гіперпов'язані мережі, що розвиваються, можуть створити єдину точку невдачі для сотень підприємств, державних установ, критичних інфраструктур і організацій охорони здоров'я. Незабаром ми

почнемо бачити шкідливі програми, повністю створені машинами на основі автоматизованого виявлення вразливостей і складного аналізу даних. Поліморфне шкідливе програмне забезпечення не є новим, але воно збирається прийняти нове обличчя, використовуючи AI для створення складного нового коду, який може навчитися ухилятися від виявлення за допомогою машинописних процедур.

4. Проблеми з ботнетом

Мільйони нових підключених споживчих пристроїв створюють широку атакуючу поверхню для хакерів, які продовжуватимуть досліджувати зв'язки між малопотужними, дещо немічними пристроями та критичною інфраструктурою, повідомив Шон Кулі, віце-президент і технічний директор веб-сайту Cisco в Сан-Хосе, штат Каліфорнія. Найбільшою проблемою безпеки, яку він бачить, є створення атак DDoS з розподіленим руйнуванням, які використовують рої погано захищених споживчих пристроїв для атаки громадської інфраструктури через масу скоординованого зловживання каналами зв'язку.

Бот-мережі IoT можуть направляти величезні рої підключених датчиків, таких як термостати або контролери дощувальних пристроїв, щоб викликати шкідливі та непередбачувані спади в інфраструктурному використанні, що призводить до таких подій, як стрибки напруги, руйнівні атаки або зменшення доступності критичної інфраструктури на рівні міста чи штату. . Рішення для цих атак існують, від більш розумного програмного забезпечення для керування, яке може визначити різницю між аварійними та помилковими датчиками даних, і стандартами, які встановлюють межі на те, що пристрої даних дозволяють відправляти, або як часто їм дозволено відправляти. Проте залишається проблемою збереження датчиків і пристроїв споживчого класу, особливо, оскільки вони пов'язуються, в масовому порядку, з нашою спільною інфраструктурою.

5. Відсутність довіри

Компанія Gemalto, розташована в Амстердамі, в Нідерландах, є фірмою з кібербезпеки, яка дослідила вплив безпеки на розвиток IoT. Якщо встановлено, що 90 відсотків споживачів не мають впевненості в безпеці пристроїв IoT. Це призводить до того, що більше двох третин споживачів і майже 80% організацій підтримують уряди, які беруть участь у забезпеченні безпеки IoT. Фактично його нещодавній звіт про стан безпеки IoT, опублікований наприкінці жовтня, показав наступні дані.

1. 96 відсотків підприємств і 90 відсотків споживачів вважають, що повинні існувати правила безпеки ІН
2. 54% споживачів володіють у середньому чотирма пристроями IoT, але лише 14% вважають, що вони знають про безпеку пристроїв IoT
3. 65 відсотків споживачів стурбовані тим, що хакер контролює їх пристрій IoT, а 60 відсотків стурбовані тим, що дані витікають

Зрозуміло, що і споживачі, і підприємства мають серйозні побоювання щодо безпеки IoT і мало впевненості в тому, що постачальники послуг IoT і виробники пристроїв зможуть захистити пристрої IoT і, що більш важливо, цілісність даних, створених, збережених і переданих цими пристроями

6. Розуміння IoT

У 2019 році справжня проблема полягає в тому, як підвищити здатність людей чіткіше зрозуміти зміни та їхні наслідки, а також зробити конкретні дії, щоб скористатися потенційним потенціалом.

Інтернет речей переходить у підлітковий вік, оскільки підключені пристрої стають розумнішими та більш захоплюючими, а також очікуванням перетворення даних IoT на розуміння та збільшення фінансової вартості. Крім того, алгоритми та шаблони візуалізації даних розвивалися таким чином, щоб нові випадки використання могли скористатися перевагами попередніх. Експоненціальне прийняття IoT призведе до зниження витрат на датчик і придбання, що дозволить все

більше і більше життєздатних бізнес-кейсів, які раніше були занадто дорогими.

7. Дані і їх складність

IoT генерує незліченні байти даних. Але це не те, як підприємства оцінюють свою цінність. Вони дивляться на аналіз тенденцій і закономірностей. Наприклад, скажімо, що один сенсор повідомляє один з десяти можливих значень щотижня. Через рік ви зможете зібрати 52 пункти даних. Але, кількість можливих комбінацій цих 52 пунктів становить 1 x 1052. Хочемо певної перспективи? Оцінка кількості атомів на всій планеті становить 1 x 1050, що в 100 разів менше. [1]

Як ми бачимо, основною і потребуючою негайного розв’язку проблемою IoT залишається безпека, одному з основних аспектів якої, а саме автентифікації і присвячена дана робота.

1.2 Автентифікація Інтернету речей

Прочитайте будь-яку статтю про Інтернет речей (IoT), і ви побачите повторювану тему, що вона не досягне свого потенціалу, якщо вона не є безпечною. Цей момент, як правило, робиться шляхом опису страшного сценарію, коли зловмисник має доступ до даних або виконує операцію, видаючи себе за дійсного користувача. Це підкреслює важливість автентифікації IoT - якщо ви не впевнені, з яким об'єктом ви обмінюєтеся повідомленнями, то не можете захистити потенційно конфіденційні дані, а також транзакції, що проводяться.

Це принципово одна і та ж вимога сьогоднішнього людсько-орієнтованого Інтернету - ми повинні бути в змозі знати, з ким ми маємо справу, купуючи подарунки на свято або твітте фотографій кошенят. Веб-сайти автентифікують користувачів, вимагаючи пароля, а веб-переглядачі перевіряють автентифікацію веб-сайтів через протокол SSL (Secure Sockets Layer). На жаль, настільки погано, як і паролі для автентифікації в Інтернет-

масштабі, вони ще гірше для автентифікації в IoT-масштабі (12-ти значний пароль з комбінацією різних символів для браслету, що лише рахує ваші кроки здається не дуже гарною ідеєю)

Щоб мати візуальне представлення розглянемо архітектуру приладів інтернету речей для охорони здоров’я :

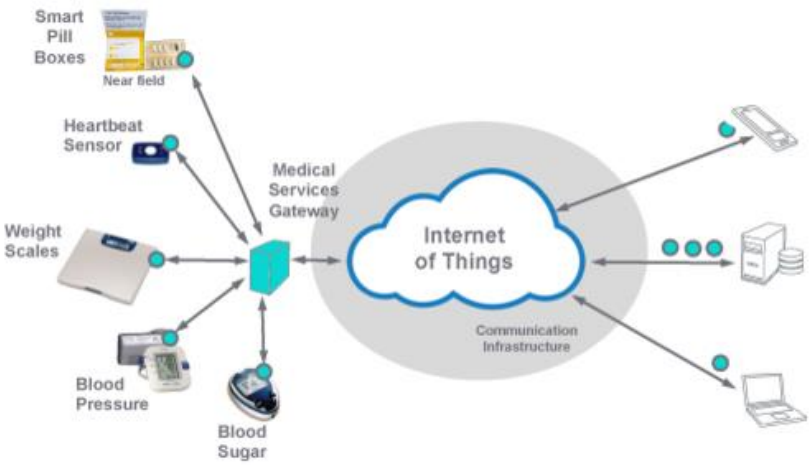

Рисунок 1.1 - Приблизна архітектура IoT приладів для охорони здоров'я [2]

1. Медичні пристрої зліва перевіряють автентичність на локальному шлюзі при передачі даних про здоров'я.
2. Шлюз потім автентифікується до кінцевої точки хмари при

пересиланні цих даних.

3. Тоді застосунки, розташовані праворуч, які аналізуватимуть та передаватимуть ці дані, повинні також перевіряти автентичність у хмарі під час запиту даних.

Єдиною масштабованою моделлю для цього сценарію автентифікації є маркери безпеки, де один учасник автентифікується іншим шляхом включення раніше отриманого маркера на свої повідомлення. Маркер служить для ідентифікації першого учасника, що дозволяє другому учаснику прийняти відповідне рішення щодо авторизації.

Для медичних даних та іншої особистої інформації важливо, щоб відповідні користувачі контролювали, як збираються, обмінюються та аналізуються їхні дані про здоров'я. Потужний механізм, який дає можливість керувати цим видом управління, вимагає, щоб користувач був активно залучений до процесу, де різним суб'єктам видаються маркери безпеки, які використовуються для подальших взаємодій. Без згоди користувача не видано жодних маркерів і не відбувається жодних автентифікованих взаємодій. Іншими словами, дані про стан здоров'я не можуть надходити.

OAuth 2.0 і OpenID Connect 1.0 - це два стандартизовані рішення для автентифікації та авторизації, які підтримують вищезгадану модель. Обидва дозволяють користувачеві брати участь у видачі маркерів для додатків, які шукають дані користувача (здоров'я або інше), що дає змогу контролювати конфіденційність. Крім того, Connect надає вбудовані механізми виявлення та реєстрації, які є надзвичайно важливими для масштабування будь-якої архітектури до кількості учасників, які створює IoT.[4]

Одна з проблем полягає в тому, що OAuth і Connect на даний момент пов'язані тільки з HTTP. Експерти з безпеки вважають, що HTTP є недостатнім для багатьох взаємодій в IoT, зокрема, між речами / пристроями та іншими суб'єктами. З'явився новий клас протоколів, який обіцяє бути більш придатним, ніж HTTP, до таких взаємодій, включаючи MQ Telemetry Transport (MQTT) і протокол обмеженого застосування (COAP). Були ранні дослідження зв'язування OAuth і Connect з цією новою категорією оптимізованих протоколів IoT, але є ще багато роботи.[5]

Завдання розробки нових механізмів і стандартів для автентифікації сторін IoT - це не вся історія. Можливість автентифікації в IoT полягає в тому, щоб визнати потенціал для створення нових способів автентифікації користувачів за допомогою пристроїв і речей, які нас оточують. Використання смартфона для двофакторної автентифікації є раннім проявом цієї тенденції. Функції, які роблять смартфон потужним фактором автентифікації, є такими ж, що дозволить нашим годинникам, браслетам і термостатам мати думку про нашу ідентичність (і здатність стверджувати цю думку).

Смартфон є потужним фактором в автентифікації, тому що для більшості користувачів він завжди знаходиться з ними (фактор "що у вас є" мало цінний, якщо ви не можете припустити, що користувачі мають його в своєму розпорядженні). Але ця якість тісно пов'язана з користувачем ще більше відповідає новому класу зносу, що використовується для моніторингу вправ, сну та інших особистих показників.

Наприклад, про браслет Fitbit. Fitbit - це крихітний підключений комп'ютер, який тісно пов'язаний з певним користувачем і дає відгук про щоденну діяльність цього користувача. Як і інші подібні пристрої, він може використовувати дані про діяльність для полегшення автентифікації

користувача при доступі до додатків, пристроїв або хмарних сервісів. Пристрій Nymi знаходиться на один крок попереду, додаючи біометричну інформацію для автентифікації користувача. Вона не зробить ключі, які вона зберігає, доступними для перевірки автентичності, до перевірки електрокардіограми власника проти збереженого шаблону.[3]

Крім носіїв, категорія пасивної автентифікації може бути включена іншими пристроями, які оточують нас. Поточні системи виявлення шахрайства використовують IP-адресу комп'ютера для виявлення атак, ініційованих з локальної мережі, що не очікується зловмисником

Тепер розглянемо конкретні способи автентифікації в IoT

1. Автентифікація за іменем користувача і паролю
2. Автентифікація по токену доступу
3. Автентифікація на основі одноразового пароля (OTP)

У додаток до основних механізмів автентифікації, можна дотримуватися необхідності реалізації додаткових механізмів захисту, щоб ідентифікувати надлишкові пристрої. У цій стадії описується підхід до реалізації в таких ситуаціях автентифікації на основі одноразових паролів (OTP). OTP-автентифікація може виявитися корисним механізмом захисту від невідповідного застосування для облікового запису доступу до неавторизованих користувачів.

У цьому випадку тільки автентифіковані користувачі можуть після запуску пристроїв розпочати обмін даними з IoT-додатками. Якщо OTP-автентифікація налагоджена, пристрій запускає запит OTP на IoT-додаток-брокера з допомогою звичайного обміну повідомленнями. Відповідна схема дій, на прикладі IBM Watsons, зображена на діаграмі (рисунок. 1.2)

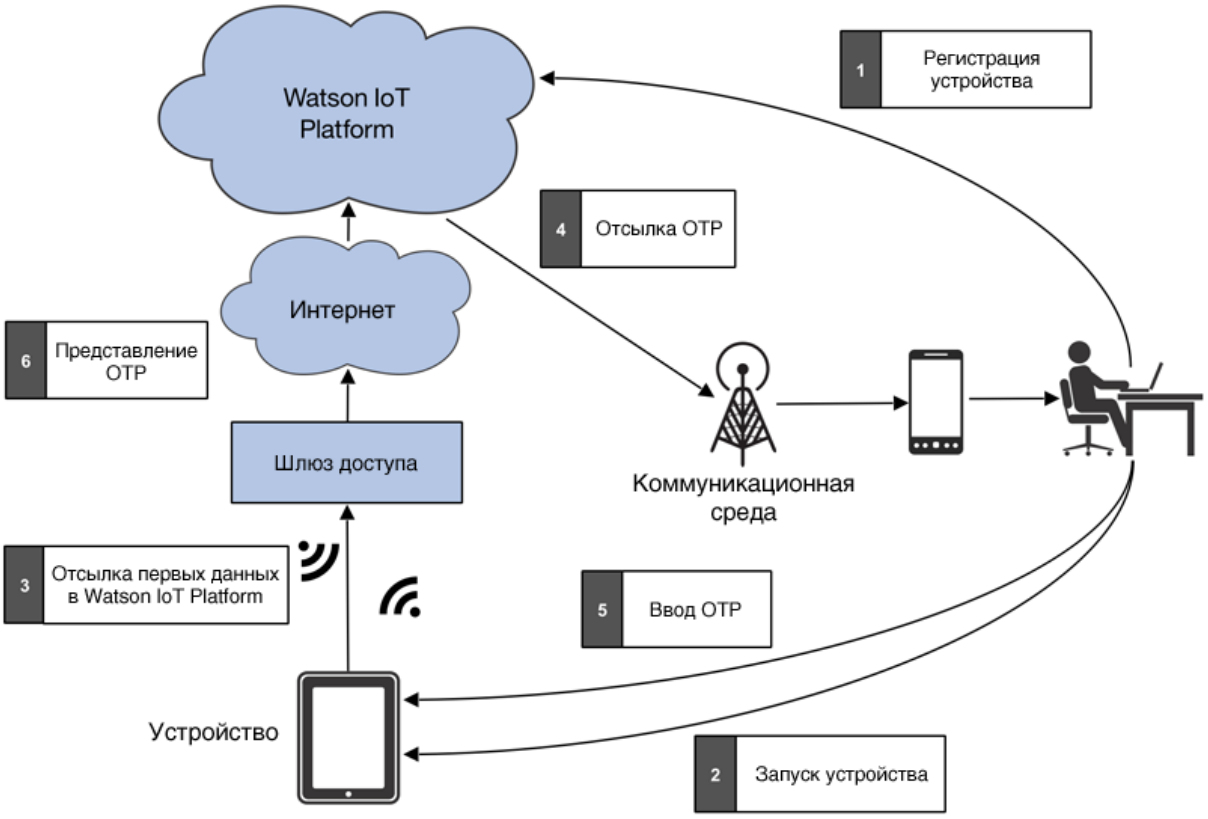

Рисунок 1.2 - Схема додаткової автентифікації засобами OTP[7]

1. Автентифікація на основі сертифікатів
2. Автентифікація на основі індивідуальних біологічних даних

1.3 Постановка задачі

Проаналізувавши поточний стан забезпечення безпеки в мережах інтернету речей я встановив, що головною проблемою в цій галузі є не відсутність ефективних методів захисту, а надзвичайно велика кількість засобів автентифікації в поєднанні з великою кількістю змінних, що належить розглянути при виборі методу, що буде оптимальним в конкретному випадку.

Отже, головною задачею даної роботи я ставлю створення математичної моделі аналізу методів автентифікації, що буде залежати від змінних, що будуть запроваджені користувачем, а також метааналіз джерел порівняння та опису різних методів захисту в IoT для створення інформаційної бази, на яку буде застосований запропонований аналітичний апарат.

Висновки до розділу 1

В ході дослідження та формування проблематики предметної області мною було виявлено, що наразі основною проблемою мереж інтернету речей є недовіра користувачів до аспекту безпеки. Під час розвитку IoT було багато прецедентів масового взлому пристроїв, створення ботнетів та інших речей, що підривають цінність таких перспективних галузей, як розумні будинки, автомобілі та інше.

Проаналізувавши питання забезпечення безпеки в IoT я дійшов висновку, що основною проблемою є перенасичення даної сфери готовими рішенням та складність вибору якогось конкретного з них, що буде ефективним в тому чи іншому випадку

ДОСЛІДЖЕННЯ БАЗИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В МЕРЕЖАХ ІНТЕРНЕТУ РЕЧЕЙ

2.1 Моделі загроз в IoT

Для подальшої роботи потрібно сформулювати модель загрози IoT

Приєднані спеціальні пристрої мають значну кількість потенційних ділянок поверхні взаємодії та схеми взаємодії, всі з яких повинні розглядатися як основи для забезпечення цифрового доступу до цих пристроїв. Термін "цифровий доступ" використовується тут, щоб відрізнити від будь-яких операцій, які здійснюються за допомогою безпосередньої взаємодії пристрою, де безпека доступу забезпечується через фізичний контроль доступу. Наприклад, помістивши пристрій в кімнату з замком на дверях. Незважаючи на те, що фізичний доступ не може бути відхилений за допомогою програмного та апаратного забезпечення, можуть бути вжиті заходи для запобігання фізичного доступу, який призводить до втручання системи.

Під час моделювання загроз і методів забезпечення безпеки IoT потрібно розглядати контроль пристрою та дані пристрою з однаковим рівнем уваги. Контроль пристрою може бути класифікований як будь-яка інформація, яка надається пристрою будь-якою стороною з метою зміни або впливу на її поведінку щодо її стану або стану його середовища. Дані пристрою можна класифікувати як будь-яку інформацію, яку пристрій видає будь-якій іншій стороні про її стан і спостережуване стан свого оточення.

Для оптимізації передового досвіду в галузі безпеки рекомендується, щоб типова архітектура IoT була розділена на декілька компонентів / зон як частину вправи для моделювання загроз. Ці зони описані в цьому розділі і включають:

1. Пристрій
2. Польові шлюзи
3. Хмарні шлюзи
4. Служби

Зони є широким способом сегментувати рішення; кожна зона часто має свої власні дані та вимоги щодо автентифікації та авторизації. Зони також можуть бути використані для ізоляції пошкоджень та обмеження впливу зон з низькою довірою на більш високі цільові зони.

Кожна зона відокремлена межею довіри, яка на нижченаведеній діаграмі (рис 1.2) позначена як пунктирна червона лінія. Вона являє собою перехід даних інформації від одного джерела до іншого. Під час цього переходу інформація може підлягати (згідно зі STRIDE): викриттю ідентичності користувача, несанкціонованому втручанню, відмові, розкриттю інформації, відмові в обслуговуванні та підвищенню привілеїв.

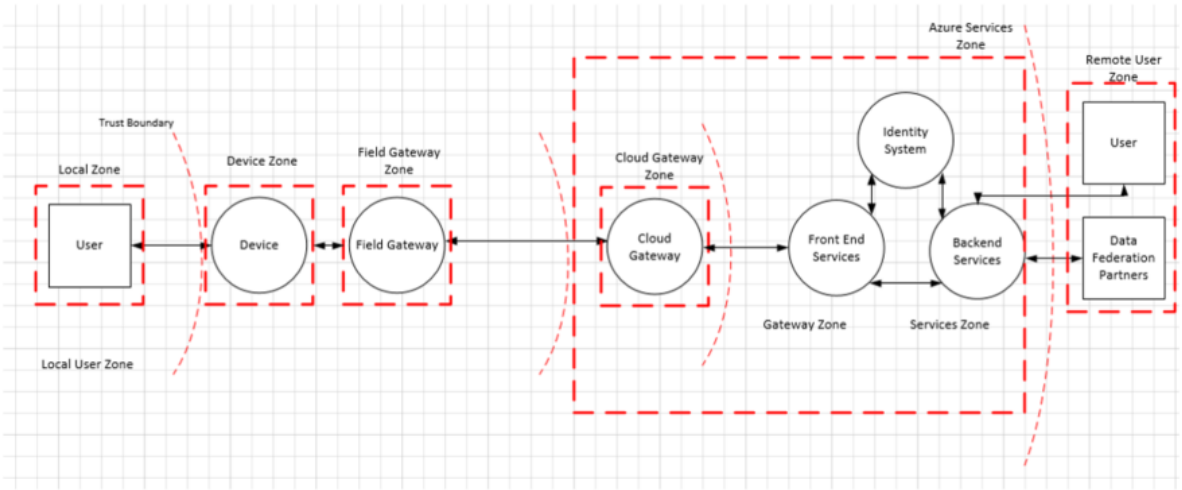

Рисунок 2. 1 - Типова модель виокремлення зон IoT[6]

Компоненти, зображені в межах кожної межі, також піддаються аналізу згідно зі STRIDE, що дозволяє отримати повний вид моделювання

загроз.

Розглянемо більше детально кожну з зон:

1. Зона пристрою

Середовище пристрою - це безпосередній фізичний простір навколо пристрою, де фізичний доступ і / або локальна мережа. Локальна мережа вважається мережею, яка відрізняється і є ізольованою від - але потенційно сполученої з - Інтернетом, і включає будь-яку технологію бездротового радіозв'язку короткого діапазону, яка дозволяє здійснювати однорангову комунікацію пристроїв. Вона не включає в себе будь-яку мережеву технологію віртуалізації, що створює ілюзію такої локальної мережі, а також не включає мережі громадського оператора, які вимагають, щоб будь-які два пристрої обмінювалися інформацією через публічний мережевий простір, якщо б вони входили в зв'язок між рівноправними.

2. Зона поля шлюзу

Поле шлюзу - це пристрій або певне серверне комп'ютерне програмне забезпечення загального призначення, яке діє як засоби забезпечення зв'язку і, потенційно, як система управління пристроєм і вузол обробки даних пристрою. Зона шлюзу поля включає в себе сам шлюз поля і всі приєднані до нього пристрої. Як випливає з назви, польові шлюзи виступають за межами спеціалізованих засобів обробки даних, зазвичай пов'язані з розташуванням, потенційно підлягають фізичному втручанню, і мають обмежену оперативну надмірність.

Польовий шлюз відрізняється від простого маршрутизатора трафіку тим, що він має активну роль в управлінні доступом і інформаційним потоком, тобто він є адресованим об'єктом і мережевим з'єднанням або сеансовим терміналом. На відміну від цього, пристрій NAT або брандмауер

не є шлюзами поля, оскільки вони не є явними терміналами з'єднання або сеансу, а швидше з'єднаннями маршрутів (або блоків) або сеансів, що здійснюються через них. Польовий шлюз має дві окремі ділянки поверхні. Один звернений до пристроїв, які прикріплені до нього і представляє внутрішню частину зони, а інший стоїть перед усіма зовнішніми сторонами і є краєм зони.

3. Зона шлюзу хмари

Шлюз хмари - це система, яка дозволяє здійснювати віддалене спілкування від і до пристроїв або польових шлюзів з декількох різних сторін через простір публічної мережі, зазвичай до системи керування та аналізу даних у хмарі. У деяких випадках хмарний шлюз може негайно полегшити доступ до спеціальних пристроїв з терміналів, таких як планшети або телефони. Також в зоні хмари операційні заходи запобігають цілеспрямованому фізичному доступу і не обов'язково піддаються інфраструктурі «публічної хмари».

Шлюз хмари потенційно може відображатися в накладенні мережевої віртуалізації, щоб ізолювати шлюз хмари та всі приєднані пристрої або шлюзи поля від будь-якого іншого мережевого трафіку. Шлюз хмари сам по собі не є системою керування пристроями або засобом обробки або зберігання даних пристрою; ці об'єкти взаємодіють з хмарним шлюзом. Зона шлюзу хмари включає в себе сам шлюз хмари разом з усіма шлюзами поля та пристроями, які безпосередньо або опосередковано приєднані до нього. Край зони - це окрема площа поверхні, через яку всі зовнішні сторони спілкуються.

4. Зона служб

Служба визначається для цього контексту як будь-який компонент або модуль програмного забезпечення, що взаємодіє з пристроями через

шлюз поля або хмари для збору та аналізу даних, а також для команд і управління. Послуги є посередниками. Вони діють під їх ідентичністю по відношенню до шлюзів та інших підсистем, зберігають і аналізують дані, автономно видають команди пристроям на основі даних або графіків даних і розкривають інформацію та можливості контролю уповноваженим кінцевим користувачам.

Проаналізувавши основні зони та загроз IoT можна побудувати наступні моделі:

- Процеси (як під нашим контролем, так і зовнішніми елементами)

Нижче наведено огляд найпоширеніших загроз для категорії "процеси", а потім - огляд того, як їх можна найкраще пом'якшити:

1. Spoofing (S)

Зловмисник може витягти матеріал криптографічного ключа з пристрою, або на рівні програмного або апаратного забезпечення, і згодом отримати доступ до системи з іншим фізичним або віртуальним пристроєм під ідентифікацією пристрою, з якого було взято ключовий матеріал. Хорошою ілюстрацією є пульти дистанційного керування, які можуть перетворювати будь-який телевізор, а також популярні інструменти жартівників.

2. Denial of Service (D)

Пристрій може бути недієздатним для функціонування або спілкування, втручаючись у радіочастоти або ріжучі дроти. Наприклад, камера відеоспостереження, яка має власну або мережеву зв'язок, навмисно вибита, не може передавати дані.

3. Tampering (T)

Зловмисник може частково або повністю замінити програмне забезпечення, що працює на пристрої, потенційно дозволяючи заміненому програмному забезпеченню використовувати справжню ідентичність пристрою, якщо ключовий матеріал або криптографічні засоби, що містять ключові матеріали, були доступні для незаконної програми. Наприклад, зловмисник може використовувати екстрагований ключовий матеріал для перехоплення і придушення даних з пристрою на шляху зв'язку і заміни його помилковими даними, які автентифікуються за допомогою викраденого ключового матеріалу.

4. Information Disclosure (I)

Якщо пристрій працює з програмним забезпеченням, що маніпулюється, таке маніпульоване програмне забезпечення може потенційно пропускати дані до сторонніх осіб. Наприклад, зловмисник може використовувати екстрагований ключовий матеріал, щоб ввести себе в комунікаційний шлях між пристроєм і контролером або шлюзом поля або шлюзом хмари, щоб відключити інформацію.

5. Elevation of Privilege (E)

Пристрій, який виконує певну функцію, може бути змушений зробити щось інше. Наприклад, клапан, який запрограмований на відкриття на половину шляху, можна обдурити, щоб відкрити весь шлях.

Ось деякі приклади загроз у цій категорії:

Спуфінг: зловмисник може витягувати матеріал криптографічного ключа з пристрою, або на рівні програмного або апаратного забезпечення, і згодом отримати доступ до системи з іншим фізичним або віртуальним пристроєм під ідентифікацією пристрою, з якого було взято ключовий матеріал.

Відмова в обслуговуванні: Пристрій може бути нездатним до функціонування або спілкування, втручаючись в радіочастоти або ріжучі дроти. Наприклад, камера відеоспостереження, яка має власну або мережеву зв'язок, навмисно вибита, не може звітувати про дані.

Несанкціоноване втручання: Зловмисник може частково або повністю замінити програмне забезпечення, що працює на пристрої, потенційно дозволяючи зміненому програмному забезпеченню використовувати справжню ідентичність пристрою, якщо ключовий матеріал або криптографічні засоби, що містять ключові матеріали, були доступні для незаконної програми.

Несанкціоноване втручання: Камера спостереження, яка показує зображення пустого коридору з видимим спектром, може бути спрямована на фотографію такого передпокою. Датчик диму або вогню може повідомляти, що хтось тримає під ним запальничку. У будь-якому випадку, пристрій може бути повністю надійним до системи, але повідомляє про маніпульовану інформацію.

Несанкціоноване втручання: Зловмисник може використати вилучений ключовий матеріал для перехоплення та придушення даних з пристрою на комунікаційному шляху і замінити його помилковими даними, які автентифікуються викраденим ключовим матеріалом.

Несанкціоноване втручання: Зловмисник може частково або повністю замінити програмне забезпечення, що працює на пристрої, потенційно дозволяючи зміненому програмному забезпеченню використовувати справжню ідентичність пристрою, якщо ключовий матеріал або криптографічні засоби, що містять ключові матеріали, були доступні для незаконної програми.

Розкриття інформації: Якщо пристрій працює з програмним

забезпеченням, що маніпулюється, таке маніпульоване програмне забезпечення може потенційно пропускати дані до сторонніх осіб.

Розкриття інформації: Зловмисник може використати вилучений ключовий матеріал, щоб ввести себе в комунікаційний шлях між пристроєм і контролером або шлюзом поля або шлюзом хмари, щоб відключити інформацію.

Відмова в обслуговуванні: Пристрій може бути вимкнений або перетворений в режим, де неможлива комунікація (яка є навмисною у багатьох промислових машинах).

Несанкціоноване втручання: Пристрій може бути переналаштовані для роботи в невідомому для системи керування стані (за межами відомих параметрів калібрування) і таким чином надавати дані, які можуть бути неправильно витлумачені

Несанкціоноване підвищення привілеї: Пристрій, який виконує певну функцію, може бути змушений зробити щось інше. Наприклад, клапан, який запрограмований на відкриття на половину шляху, можна обдурити, щоб відкрити весь шлях.

Відмова в обслуговуванні: Пристрій може бути перетворено в стан, де зв'язок неможливий.

Несанкціоноване втручання: Пристрій може бути переналаштований для роботи в невідомому для системи управління стані (за межами відомих параметрів калібрування) і таким чином надавати дані, які можуть бути неправильно інтерпретовані.

Порушення / несанкціоноване втручання / відхилення: Якщо не захищено (що рідко буває у випадку дистанційного керування для споживачів), зловмисник може анонімно маніпулювати станом пристрою.

Хорошою ілюстрацією є пульти дистанційного керування, які можуть перетворювати будь-який телевізор, а також популярні інструменти жартівників.

- Зв’язок

Загрози навколо шляху зв'язку між пристроями, пристроями та шлюзами поля та шлюзом пристрою та хмари.

Ось деякі приклади загроз у цій категорії:

Відмова в обслуговуванні: обмежені пристрої зазвичай перебувають під загрозою DoS, коли вони активно слухають вхідні з'єднання або небажані дейтаграми в мережі, оскільки зловмисник може паралельно відкривати багато з'єднань і не обслуговувати їх або повільно обслуговувати, або пристрій може бути затоплений небажаний трафік. В обох випадках пристрій може бути ефективно виведено з ладу в мережі.

Викриття, розкриття інформації: обмежені пристрої та спеціальні пристрої часто мають засоби безпеки один-на-все, такі як захист паролем або PIN-кодом, або вони повністю покладаються на довіру до мережі, тобто вони надають доступ до інформації, коли пристрій перебуває в одній мережі і ця мережа часто захищається лише спільним ключем. Це означає, що, коли розкривається спільний секрет пристрою або мережі, можна керувати пристроєм або спостерігати дані, що випускаються з пристрою.

Спуфінг: зловмисник може перехопити або частково перевизначити трансляцію і підмінити автора (людина посередині)

Несанкціоноване втручання: зловмисник може перехопити або частково перекрити трансляцію і надіслати неправдиву інформацію

Розкриття інформації: зловмисник може підслуховувати трансляцію

та отримувати інформацію без дозволу «Відмова в обслуговуванні»: зловмисник може заклинити передачу сигналу та заборонити розповсюдження інформації

- Сховища

Кожен пристрій і шлюз поля мають певну форму сховищ (тимчасове для зберігання даних, операційна система (ОС) зберігання зображень).

Зона обробки пристроїв і подій / хмара

Шлюз хмари - це система, яка дозволяє віддалене спілкування від і до пристроїв або польових шлюзів з декількох різних ресурсів через простір публічної мережі, зазвичай до системи керування та аналізу даних у хмар. У деяких випадках хмарний шлюз може негайно полегшити доступ до спеціальних пристроїв з терміналів, таких як планшети або телефони. У контексті, що обговорюється тут, "хмара" позначається на спеціальній системі обробки даних, яка не пов'язана з тим самим ресурсом, що й прикріплені пристрої або польові шлюзи, і де операційні заходи запобігають цілеспрямованому фізичному доступу, але не обов'язково до “ інфраструктури громадської хмари. Шлюз хмари потенційно може відображатися в накладенні мережевої віртуалізації, щоб ізолювати шлюз хмари та всі приєднані пристрої або шлюзи поля від будь-якого іншого мережевого трафіку. Шлюз хмари сам по собі не є системою керування пристроями або засобом обробки або зберігання даних пристрою; ці об'єкти взаємодіють з хмарним шлюзом. Зона шлюзу хмари включає в себе сам шлюз хмари разом з усіма шлюзами поля та пристроями, які безпосередньо або опосередковано приєднані до нього.

Хмарний шлюз - це в основному користувацька частина програмного забезпечення, що працює як служба з відкритими кінцевими точками, до яких підключається шлюз поля та пристрої. Як така, вона повинна бути

розроблена з урахуванням безпеки.

Зона послуг

Система управління (або контролер) - це програмне рішення, яке взаємодіє з пристроєм або шлюзом поля, або хмарним шлюзом з метою керування одним або кількома пристроями та / або для збору та / або зберігання та / або аналізу даних пристрою для презентації або подальшого контролю. Системи контролю є єдиними суб'єктами в рамках цієї дискусії, які можуть негайно сприяти взаємодії з людьми. Виняток становлять проміжні фізичні поверхні управління на пристроях, такі як перемикач, який дозволяє людині вимикати пристрій або змінювати інші властивості, і для яких немає функціонального еквівалента, до якого можна отримати доступ цифровим способом.

Проміжні фізичні поверхні управління - це ті, де керуюча логіка обмежує функцію фізичної поверхні управління таким чином, що еквівалентна функція може бути ініційована дистанційно або можна уникнути конфліктів вхідного сигналу з віддаленим введенням - такі посередні поверхні керування концептуально приєднані до локальної системи управління, яка використовує таку ж функціональність, як і будь-яка інша система дистанційного керування, до якої пристрій може бути приєднаний паралельно.

2.2 Існуючі моделі автентифікації в IoT

1. RFID та NFC

Радіочастотна ідентифікація (RFID) - це бездротова технологія, яка складається з тегів, які можуть бути прикріплені до будь-якого фізичного об'єкта або навіть до людей; його основною метою є виявлення або

виявлення об'єктів з тегами. RFID може бути розгорнутий у різних областях, наприклад, у ланцюжку постачання, охороні здоров'я, зондування клімату тощо. В [23] автори запропонували простий протокол автентифікації для RFID-міток на основі PUF.

Протокол складається з трьох транзакцій: розпізнавання тегів, перевірка та оновлення. У першій транзакції, читач тегів розпізнає тег. Друга транзакція - це перевірка, де читач і тег взаємно перевіряють автентичність один одного. В останній транзакції (Оновлення), для наступної перевірки слід зберігати останній використаний ключ. Для захисту ланцюжка поставок підключених пристроїв автори [23] включили автентифікацію і сприйняття пристроїв IoT через рішення на основі RFID. Процес автентифікації складається двох кроків: перевірка зв'язку між тегом і пристроєм IoT, а потім затвердження сприйнятливість мітки. У системі на основі IoT-RFID зчитувач RFID підключається до Інтернету для формування кінця IoT пристрою. З іншого боку, він з'єднаний з позначеними елементами за допомогою протоколів зв'язку RFID.

Елемент з тегами є портативним і переміщується від читача до іншого, таким чином існує потреба в перевірці ідентичність один одного за допомогою автентифікації. Через відсутність криптографічних функцій у RFID, система є вразливою до загроз безпеки, таких як арешти або клонування. В [23] автори представив протокол автентифікації, який буде використовуватися у випадку використання IoT-RFID з використанням легкого ваги алгоритм шифрування. Щоб протистояти клонуванню атак до мітки RFID, автори [24] запропонували автономний режим автентифікації для RFID-міток на основі PUF. Він поєднував як ідентифікацію, так і цифровий підпис протоколи безпеки. Під час автентифікації тег генерує секретний ключ, оскаржуючи PUF і збір відповіді. Така відповідь з допомогою допоміжних даних створить сертифікат, який буде зберігатися

всередині ROM тега. Потім верифікатор автентифікує тег, перевіряючи правильність сертифікат. Для забезпечення анонімної автентифікації для систем RFID автори [25] представили а Схема автентифікації на основі PUF для класичних міток RFID. Потім вони забезпечили розширену схему шумна середовище PUF. Головним недоліком такої схеми є не врахування повторної відправки на сервер з новою парою Challenge – Response Pair (CRP), коли існуючий пул стає порожнім.

Автори [26] запропонували двофакторну схему автентифікації на основі смартфона з Near. Функція Field Communication (NFC) є першим чинником і відбитком пальця користувача як другого фактора. Обидва фактори використовуються для автентифікації користувача в системі смарт-бібліотеки. База даних бібліотеки перевіряє особисті дані, вбудовані в тег NFC, і збіг відбитків пальців, до яких користувач має право доступ до внутрішньої бібліотечної мережі для запиту книг і надання користувачеві позиції стійки (розташування), в якому знаходиться книга. Автори [31] запропонували схему взаємної автентифікації для додатків на основі IoT RFID мобільні мережі п'ятого покоління (5G), надаючи читачеві кеш-пам'ять, для зберігання ключів (використовується для автентифікації) для нещодавно відвіданих тегів, щоб прискорити автентифікацію, зменшити обчислення вартість і підвищення безпеки при зберіганні. Автори [27] запропонували схему взаємної автентифікації для додатків на базі NFC на основі IoT 5G. Використовуючи тільки (легкі) операції Shift та XOR, щоб відповідати характеристикам продуктивності та зберігання з тегів NFC, вони надавали анонімність тегів, використовуючи псевдонім, а не справжню ідентичність.

2. Автомобільні мережі

Автомобілі в даний час пов'язані з Інтернетом або Інтернетом речей,

щоб сформувати те, що називається транспортні мережі або Інтернет транспортних засобів. Таке підключення використовується для надання різних послуг:

1. надання інформації про дорожній рух для користувачів,
2. обмін послугами катання,
3. зарядки електричних автомобілів

Електричні транспортні засоби (EV) стають тенденцією і автентифікація автомобіля є складною темою в EV систем. Автори [31] запропонували двофакторну схему автентифікації для EV, хоча вона може бути розгортаються в різних областях. Схема поєднує унікальну контекстну функцію. Автомобіль підключений за допомогою безпроводового з'єднання та зарядного пристрою через зарядний кабель, тому це залежить від фізична зв'язок для перевірки ідентичності. Автори [32] запропонували протокол автентифікації, який називають розподіленим агрегатом автентифікацію, що зберігає конфіденційність (DAPPA), яка може бути використана для автентифікації системи транспортного засобу з використання багаторазового довіреного органу одноразової ідентичності на основі сукупної техніки підпису. Автомобіль може перевіряти багато повідомлень одночасно, а їхні підписи можуть бути об'єднані в одну повідомлення, яке зменшує простір для зберігання, необхідний для транспортного засобу або збирача даних. Крім того, в [33], автори запропонували протокол автентифікації зв'язку в безпечних транспортних мережах (VANETs), використовуючи сукупні підписи на основі ідентичності. В роботі [34] автори наводили схему автентифікації за мовленням, яка називається прогнозованою Автентифікація (PBA), яка захищає від DoS-атак і протистоїть втраті пакетів. Протокол базується на конструкції хеш-дерев Меркле для миттєвої перевірки термінових повідомлень і самостійного генерування Зберігання коду автентифікації повідомлення (MAC) замість

збереження всіх підписів, що приймають. Як вдосконалення схеми в [31], автори [32] надали автентифікацію на основі передбачення (PBA) як схеми автентифікації трансляції в VANET. Запропонована схема використовує як еліптичний Підписи кривої цифрового алгоритму підпису (ECDSA) і толерантний до втрати часу потік потоків Автентифікація (TESLA) для автентифікації повідомлень між транспортними засобами, які виявилися ефективними, ефективною і схемою автентифікації. В [33], удосконалення методів подвійної автентифікації та керування ключами у VANETs запропоновано, забезпечуючи фазу автентифікації вперше, коли транспортний засіб входить в мережу і фаза повторної автентифікації, коли транспортний засіб переходить від однієї зони покриття до іншої без необхідності переглядати весь процес перевірки. Автори [33] забезпечили взаємну автентифікацію між транспортними засобами, використовуючи виклик протоколу автентифікації рукостискання (CHAP), який забезпечує автентифікацію та авторизацію, таким чином дозволяючи зарядженню транспортного засобу (V2V), використовуючи вузол конвертерного кабелю. Автори [35] запропонували протокол автентифікації для забезпечення виклику VANETs

3. Розумні будинки

Розумні будинки - це автоматизовані будинки, де користувачі будуть мати можливість контролювати, контролювати і віддалений доступ (за допомогою мобільного телефону (мобільного додатку) або персонального комп'ютера (веб-додаток)) кліматичні системи (опалення та кондиціонування повітря), побутова техніка, освітлення, телебачення, аудіо- та відеосистеми тощо. Автори [14] розробили схему безпеки, яка може бути розгорнута в розумних будинках. Такий підхід має можливість подолати деякі загрози безпеці, такі як атака на імпресіонацію та відтворення [16], але це так все ще вразливі до підслуховування. Підхід

базується на протоколі OAuth 2.0. В [41] автори представила нову схему автентифікації для автентифікації кінцевих пристроїв, розгорнутих у розумних будинках, яка заснована на комбінації PUF і фізичної генерації ключових (PKG). PUF забезпечує безпеку системи шляхом створення безпечного ключа на основі фізичних параметрів кінця пристрій (конструкція ПУФ залежить від загальної схеми виготовлення функцій, що надають їй пожливість створити унікальний секретний ключ). Повідомлення Машина-машина» (M2M) займає провідну позицію в Розвиток IoT, але він також має проблеми безпеки. В [41]ї автори розробили схему дозволяючи віддаленому користувачеві розумної домашньої мережі спілкуватися з кінцевими пристроями. Схема дозволяє:

1. взаємна автентифікація між сторонами
2. встановлювати конфіденційність даних.

Автори [42] запропонували протокол взаємної автентифікації для кінцевих пристроїв IoT (розумний корпус) на основі PUF. Вони запровадили поняття життя об'єкта циклу (OLC) для опису дорожньої карти кінцевого пристрою від виробництва до розгортання в системі IoT та опис проблем безпеки під час цієї дорожньої карти. Автори [43] розробили схему автентифікації на основі PUF для пристроїв IoT взаємної автентифікації між кінцевим пристроєм і шлюзом за допомогою даних CRP, що зберігаються всередині шлюзу. Вона також надає можливість користувачеві (смартфону або носінному пристрою) автентифікувати себе за допомогою шлюзу для того, щоб мати можливість спілкуватися з кінцевими пристроями, використовуючи генерований сеансовий ключ між ними. Дані часової мітки використовуються користувачем для забезпечення безпеки від атак повторного відтворення. Автори [44] запропонували взаємну автентифікацію для систем IoT. Схема заснована на легкі можливості протоколу обмеженого застосування (CoAP) як протоколу прикладного

рівня для зв'язок між клієнтом і сервером. Безпечний канал зв'язку забезпечується перевагою шифру Advanced Encryption Standard (AES).

4. Бездротові сенсорні мережі

Бездротові сенсорні мережі (WSN) - це можливість додавати функції підключення та зондування мільярди датчиків, вбудованих в різні області (прилади в будинках, транспортні засоби, сітки тощо). Автори [108] запропонували протокол автентифікації на підшарі контролю доступу до медіа називається Оптимізація зв'язку для спеціальних надійних промислових мереж (OCARI), в яких вони використовували одноразовий спільний ключ сеансу. Цей метод підходить для пристроїв, обмежених ресурсами. Розглянуто відповідну схему розподілу ключів Blom [109] і поліноміальну схему [110] використовуються в якості ключових протоколів управління для деяких випадків використання IoT. Автори [111] запропонували вдосконалений протокол автентифікації та керування ключами для WSNs з використанням біо-хешування [112]. Використання логічної логіки (логіка віри і дії, що забезпечує її частина зв'язку вважає, що ключ в автентифікації хороший) забезпечує взаємну автентифікацію. Автори [113,114] запропонували взаємну автентифікацію, яка складається з двох етапів: в етап реєстрації, кожен вузол повинен бути ідентифікований в системі, і на етапі автентифікації, кількість кінцевих повідомлень обмінюється між кінцевим пристроєм і сервером - це сеансовий ключ, який використовується для майбутнього спілкування. Автори [115] розробили метод групової автентифікації в бездротових мережах досягнення як взаємної автентифікації, так і конфіденційності. Кінцевий вузол буде мати можливість переміщатися між ними точки доступу без необхідності повторної автентифікації кожного разу. Всі члени роумінг-групи інформація передається на базову станцію (BS) в перший раз, коли мобільна станція (MS) автентифікована. Потім MS посилає інформацію менеджеру

групи, яка агрегує всю інформацію і відправляє його назад до BS. БС надсилає його в мережу послуг доступу для перевірки автентифікації. Проаналізувавши деякі існуючі протоколи на основі хаотичних карт, автори [116] надали хаотичний характер на основі взаємної автентифікації на основі WSN.

5. Мобільна мережа та програми

Щоб дозволити віддаленим користувачам отримувати доступ до Інтернет-послуг в будь-який час, в будь-якому місці, автори [128] запропонувала нову схему для забезпечення безпечного роумінгу для анонімних користувачів, які користуються перевагами метод підпису групи. Вони називають її умовним збереженням конфіденційності з доступом зв'язування (CPAL). В [129] автори запропонували дві схеми автентифікації, перша з яких заснована на псевдовипадковій автентифікації, а друга заснована на автентифікації з нульовим знанням забезпечення схеми автентифікації та збереження конфіденційності для LTE-A. Схеми включають всі об'єкти в мережах LTE-A взаємно автентифікують один одного і оновлюють своє місцезнаходження без за участю абонентського сервера. Автори [130] також забезпечили групову автентифікацію схема для LTE-мереж шляхом розробки групового тимчасового ключа. Вона базується на обох еліптичних кривих Діффі – Хеллман (ECDH), що забезпечує таємницю вперед і назад, використовуючи асиметричний ключ протоколу для забезпечення конфіденційності користувача. Автори [131] запропонували SEGR для автентифікації а пристроїв, що використовують обидві системи 3GPP або WIMAX. Він базується на сукупній підписи без сертифіката запропоновано усунути ускладнення управління сертифікатами в криптографії відкритих ключів. Завдяки складним питанням розробки зручної схеми автентифікації для смартфонів середовище, де сенсорний екран є найбільш зручним для

периферійних пристроїв введення, автори [132] надала процес автентифікації для пристроїв Android для смартфонів з використанням двофакторної автентифікації називається (Duth). Протокол складається з етапу реєстрації, в якому місце і час користувача вводяться шаблони на сенсорний екран зберігаються, а потім збережені дані використовуються як подвійні фактори для автентифікації. Цей підхід дозволяє підвищити безпеку без додавання додаткового обладнання. Автори [133] запропонували нову схему автентифікації для користувачів мобільних телефонів поведінковий візерунок. Вони почалися зі збору поведінки користувача мобільного телефону щодо додатки, що використовуються в певний час і тривалість використання, а потім вони змінюють ці дані на а унікальний шаблон для використання в якості автентифікації між користувачем і мобільним телефоном схема буде використовуватися як доповнення до існуючих схем автентифікації, наданих мобільним пристроєм телефони (PIN-код, відбитки пальців, жести тощо)

6. Загальні програми IoT

Автори [134] надали протокол для здійснення автентифікації між користувачем і а не між кінцевими пристроями. Це двоетапна перевірка на пристрої IoT. Пароль або а загальний секретний ключ розглядається як перший фактор автентифікації і використання PUF як другого фактор автентифікації. У зв'язку з великою кількістю пристроїв, які бажають отримати доступ до мережі, що призводить до перевантаження для сервер автентифікації і для досягнення взаємної автентифікації та безпечного керування ключами Пристрої, обмежені ресурсами, автори [135] забезпечували групову легку автентифікацію та ключова схема угоди називається GLARM. GLARM складається з двох основних етапів: а етап ідентифікації і етап групової автентифікації та узгодження ключів на основі комбінації код автентифікації повідомлення групи пристроїв, що

підлягають автентифікації. У роботі [136] автори запропонували протокол автентифікації для полегшеного пристрою для систем IoT динамік-мікрофон (S2M). Ця схема забезпечує автентифікацію на відстані між бездротовим IoT пристроїв. Реалізовано в мобільних телефонах і ПК для перевірки його експериментальних результатів

2.3 Аналіз конфіденційності в протоколах IPsec и TLS

Secure IP (IPSec) - це стандартний набір протоколів Internet Engineering Task Force (IETF) між двома точками зв'язку через мережу IP, що забезпечують автентифікацію, цілісність і конфіденційність даних. Він також визначає зашифровані, розшифровані та автентифіковані пакети. У ньому визначені протоколи, необхідні для безпечного обміну ключами та керування ключами.

IPsec можна використовувати для виконання таких дій:

1. Для шифрування даних прикладного рівня.
2. Забезпечити безпеку маршрутизаторів, які надсилають дані маршрутизації через загальнодоступний Інтернет.
3. Щоб забезпечити автентифікацію без шифрування, шляхом перевірки автентичністі, що дані походять від відомого відправника.
4. Для захисту мережевих даних шляхом налаштування схем з використанням IPsec тунелювання, при якому всі дані передаються між двома кінцевими точками, зашифровується, як і при підключенні віртуальної приватної мережі (VPN).

Компоненти IPSec:

1. Інкапсулювання корисного навантаження безпеки (ESP - Encapsulating Security Payload) - забезпечує цілісність даних, шифрування, автентифікацію та анти-відтворення. Він також забезпечує автентифікацію для корисного навантаження.
2. Заголовок автентифікації (AH - Authentication Header) - Він також

забезпечує цілісність даних, автентифікацію і анти-відтворення, і не забезпечує шифрування. Захист від анти-відтворення захищає від несанкціонованої передачі пакетів. Це не захищає конфіденційність даних.

Рисунок 2.2 - Структура використання AH[[15]

- Обмін ключами в Інтернеті (IKE - Internet Key Exchange)

Це протокол мережевої безпеки, призначений для динамічного обміну ключами шифрування і знаходження шляху над Security Assocaition (SA) між 2 пристроями. Асоціація безпеки (SA) встановлює спільні атрибути безпеки між 2 об'єктами мережі для підтримки безпечного зв'язку. Протокол керування ключами (ISAKMP) та асоціація Internet Security, яка забезпечує основу для автентифікації та обміну ключами. ISAKMP розповідає про те, як налаштування асоціацій безпеки (SA) і як прямі з'єднання між двома хостами, які використовують IPsec. Інтернет-обмін ключами (IKE) забезпечує захист вмісту повідомлень, а також відкритий кадр для реалізації стандартних алгоритмів, таких як SHA і MD5. Користувачі алгоритму IPsec створюють унікальний ідентифікатор для кожного пакета. Цей ідентифікатор дозволяє пристрою визначати, чи був пакет правильним чи ні. Пакети, які не дозволені, відкидаються і не передаються в приймач.

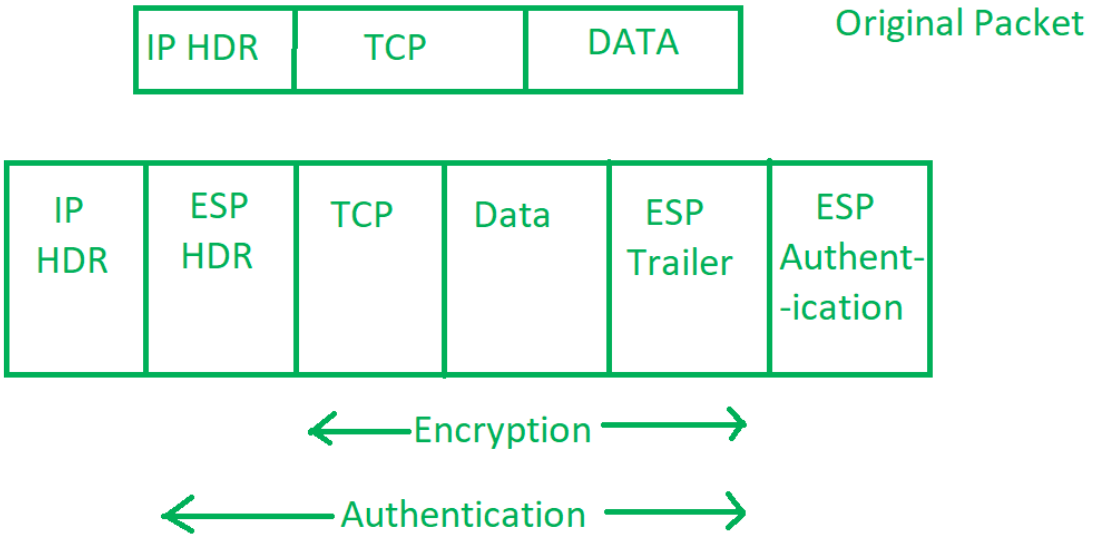

Рисунок 2.3 - Структура IPSec пакету [15]

Процес роботи IPSec:

1. Хост перевіряє, чи слід передати пакет за допомогою IPsec або ні. Цей пакетний трафік ініціює політику безпеки для себе. Це робиться, коли система, що відправляє пакет, застосовує відповідне шифрування. Вхідні пакети також перевіряються хостом, що вони правильно зашифровані.
2. Потім починається фаза IKE 1, в якій 2 хости (використовуючи IPsec) автентифікують один одного, щоб запустити захищений канал. Він має 2 режими. Головний режим, який забезпечує більший захист і агресивний режим, який дозволяє хосту швидше встановлювати IPsec-схему.
3. Канал, створений на останньому кроці, потім використовується для надійного узгодження способу, коли IP-схема буде шифрувати дані через IP-схему.
4. Тепер фаза 2 IKE проводиться по безпечному каналу, в якому два хости обговорюють тип криптографічних алгоритмів, які будуть використовуватися на сеансі, і узгодження секретного матеріалу,

який буде використовуватися з цими алгоритмами.

5. Потім дані обмінюються по новоствореному IPsec зашифрованому тунелю. Ці пакети шифруються та розшифровуються хостами за допомогою IPsec SA.
6. Коли зв'язок між хостами завершена або сеанс закінчиться, то тунель IPsec припиняється шляхом відкидання ключів обома хостами.

Тепер розглянемо TLS. TLS є криптографічним протоколом, який забезпечує комплексну безпеку зв'язку по мережах і широко використовується для інтернет-комунікацій і онлайн-транзакцій. Це стандарт IETF, призначений для запобігання підслуховуванню, цілісності та підробці повідомлень. Загальні програми, що використовують TLS, включають веб-браузери, месенджери, електронну пошту та голосовий зв'язок через IP.

Багато підприємств використовують TLS для захисту всіх комунікацій між веб-серверами та браузерами, незалежно від того, чи передаються конфіденційні дані.

Попередник TLS, secure socket layer (SSL), був розроблений Netscape в 1995 році. SSL версії 1.0 і 2.0 містили багато недоліків безпеки, що спонукало до повної переробки протоколу. У 1996 році Netscape випустила SSL версію 3.0, яка стала основою для TLS1.0. У 1999 році Рада PCI запропонувала можливе знецінення SSL як TLS 1.0 було значним оновленням до SSL 3.0.

TLS є більш ефективним та безпечним, ніж SSL, оскільки має більш сильну автентифікацію повідомлень, генерацію ключових матеріалів та інші алгоритми шифрування. Наприклад, TLS підтримує попередньо розділені ключі, захищені віддалені паролі, ключі еліптичної кривої і Kerberos, тоді як SSL - не. TLS і SSL не сумісні, але TLS пропонує зворотну сумісність для старих пристроїв, які використовують SSL.

Специфікація протоколу TLS визначає два шари. Протокол запису TLS забезпечує безпеку підключення, а протокол TLS рукостискання дозволяє клієнту і серверу автентифікувати один одного і обговорювати ключі безпеки до передачі будь-яких даних.

Рукостискання TLS - це багатоетапний процес. Базове рукостискання TLS передбачає, що клієнт і сервер посилають повідомлення "привіт", а також обмін ключами, шифрувальним повідомленням і фінальним повідомленням. Багатокроковий процес - це те, що робить TLS достатньо гнучкою для використання в різних додатках, оскільки формат і порядок обміну можуть бути змінені.

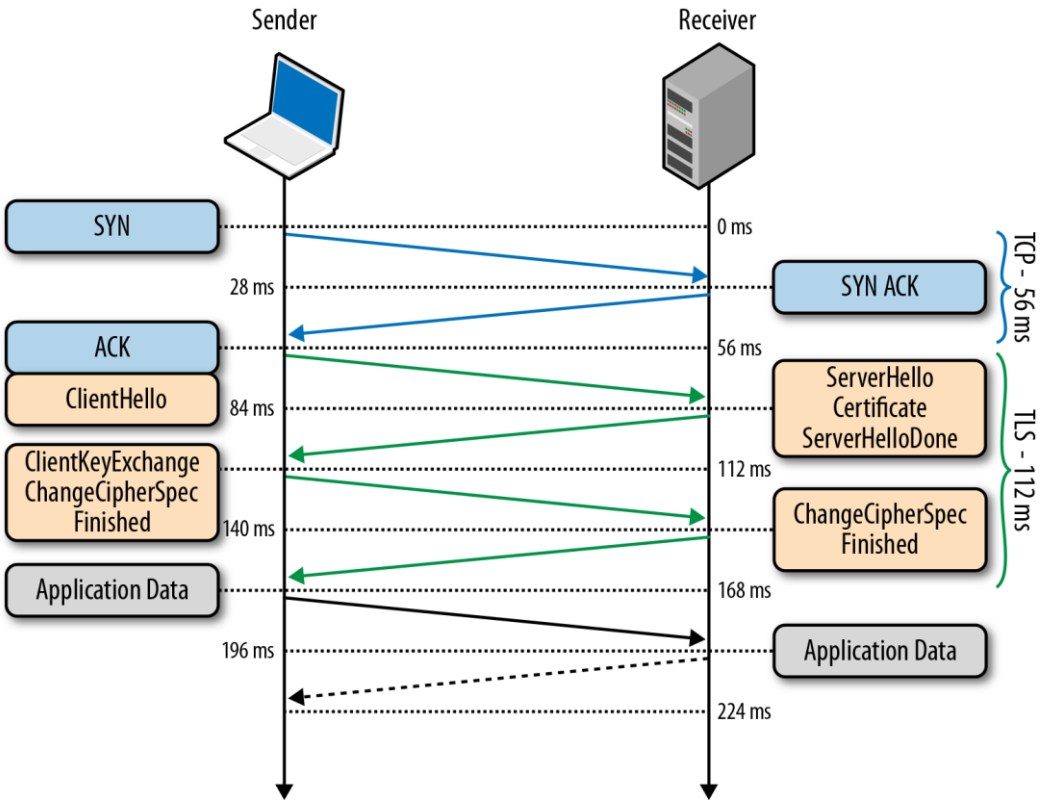

Рисунок 2.4 - Схема рукостискань TCP+TLS[17]

Порівняння протоколів IPSec та TLS:

1. Складність реалізації та покриття стандартами

В плані реалізації, TLS простіше, ніж IPsec, інтегрувати з SIP. RFC 4346

пред'являє близько 200 вимог до реалізації TLS. З іншого боку, IPsec має більше 500 вимог, що визначають реалізацію і описаних приблизно в 11 RFC.

IETF опубліковано кілька документів про те, як можуть бути інтегровані SIP, TLS і SRTP. Реалізація обох підходівможе бути неможливою, в залежності від постачальника і типу пристрою. Наприклад, деякі кінцеві пристрої обмежені в пам'яті, розмір сховища даних і обчислювальної здатності і можуть не підтримувати одночасно реалізації TLS, SRTP і IPsec.

2. Підтримка ієрархічної сигналізації

Основний маркетингової особливістю IPsec є те, що він забезпечує наскрізне шифрування, що і потрібно більшості додатків, що працюють з даними. Проте, комерційні пропозиції передачі голосу засновані на ієрархічній моделі сигналізації, в якій ОУ (термінал) оповіщає LCC (Local Call Controller), з метою встановлення сеансу зв'язку, за власним протоколу сигналізації. LCC, як правило, сповіщає SS (Software Switch) провайдера, використовуючи SIP, для виходу в зовнішню мережу, далі, SS може сповіщати інший SS або LCC з метою завершення встановлення сеансу зв'язку з віддаленим ОУ, як це показано на малюнку нижче (зліва) . Власний протокол сигналізації використовується між ОУ та LCC для того, щоб постачальник послуг міг надавати користувачеві унікальні функції з доданою вартістю, що неможливо, якщо був прийнятий стандартизований протокол.

В ієрархічній моделі, кожен хоп ієрархії повинен бути здатний розшифрувати сигнальний пакет, обробити і перешифрувати його перед відправкою. Це йде в розріз з наскрізною моделлю безпеки. Проте, і IPsec і TLS можуть бути реалізовані в рамках ієрархічної моделі, однак, в даний час, постачальники VoIP вважають, що TLS краще підходить до цієї моделі.

Наскрізна модель безпеки використовується для огранізації каналу

передачі даних і може бути реалізована, використовуючи як SRTP, так і IPsec. IEFT опублікований спосіб обміну ключмі для SRTP через SIP-пакети, таким чином, сеанс зв'язку може бути встановлений після завершення сигналізації. Схожий підхід може бути розроблений і для IPsec, але цього, в даний час, не зроблено.

3. Ефективність використання смуги пропускання

Порівняння ефективності смуги пропускання має сенс по відношенню до каналу передачі голосових даних, так як вплив пакетів сигналізації по відношенню до пакетів з даними, на смугу пропускання, незначно.

Порівнювати розмір пакетів IPsec з SRTP досить важко, оскільки вони залежать від використовуваного режиму (транспортний або тунельний), кількість байт заповнення (padding), використовуваних алгоритмів автентифікації і контролю цілісності. Прийнявши, що протокол ESP (Encapsulating Security Payload) в IPsec використовується в транспортному режимі з мінімальним заповненням і малим розміром имитовставки, можна стверджувати, що SRTP на 6% більше ефективний для IPv6-пакетів, ніж IPsec. Якщо потрібно контролювати цілісність IP-заголовка, то в IPsec може бути використаний протокол AH (Authentication Header), що спричинить за собою появу додаткових накладних витрат.

4. Комерційне застосування

Комерційні постачальники послуг вкладають серйозні кошти в використання TLS і SRTP, для забезпечення безпек. IPsec так само розглядався для цього завдання, однак TLS і SRTP були визнані кращим рішенням. На даний момент не існує комерційної реалізації IPsec, призначеної для забезпечення безпеки заснованої на SIP. Постачальники, які використовують legacy-сигналізацію H.323 для своїх рішень передачі

голосу, швидше за все, виберуть IPsec для захисту своїх рішень. Однак більшість постачальників H.323, в даний час, використовують рішення без шифрування і переходять до рішень, заснованим на SIP.

5. Information Assurance

Найбільш поширений аргумент на користь використання IPsec полягає в тому, що він забезпечує наскрізне шифрування. Однак, ця перевага не використовується в разі сигналізації, оскільки більшість реалізацій засновані на, як говорилося раніше, ієрархічної моделі сигналізації, а TLS краще підходить для цієї моделі.

Перевага IPsec полягає в тому, що він захищає дані на мережевому рівні IP, що нижче в стекупротоколів, ніж TLS, який забезпечує захист на транспортному рівні.

Іншою відмінністю між IPsec і SRTP є те, що IPsec зашифровує заголовок RTP, в той час як SRTP цього не робить. Перевага використання IPsec тут в тому, що він приховує корисну інформацію від потенційного зловмисника. Недолік полягає в тому, що це обмежує здатність міжмережевих екранів і SBC (Session Border Controllers) в застосуванні микроканалов на певних портах. Це стає особливо критичним для міжмережевих екранів і SBC виступаючих в ролі пристроїв перетворення мережевих адрес (NAT) для декількох перекриваються LCC. Оскільки IP-адреси всіх, хто прибуває пакетів спрямовані на міжмережевий екран або SBC, єдиною відмінною рисою, яку екран або SBC можуть використовувати для визначення відповідного цільового LCC, це номер порту.[19]

Обидва протоколу використовують схожі механізми шифрування, автентифікації і контролю цілісності. Наприклад, обидва протоколи підтримують шифрування з використанням відкритих ключів, симетричне шифрування AES і імітозащіти HMAC-SHA1. Таким чином, з цієї точки зору різниця в безпеці відсутня.

6. Установка з'єднання, зміна ключів і час відновлення зв'язку

Для уникнення надмірно довгого часу створення сеансу і ефекту відсічення (втрати пакетів на початку сеансу голосового зв'язку) вкрай важливо, що б ключ шифрування каналу передачі даних був поширений як частина процесу сигналізації. IEFT визначило спосіб поширення ключів SRTP як частини SIP сигналізації, поміщаючи ключ в тіло SDP (Session Description Protocol) SIP-повідомлення. IEFT на даний момент не розроблений механізм SDP поширення ключів шифрування в IPsec. Більш того, модель запит / відповідь з RFC 3264 може перешкоджати включенню ключової інформації IPsec в сигнальні повідомлення SIP.[20]

Інше питання це затримка, пов'язана зі зміною ключів. Недавні дослідження, в яких порівнюється час зміни ключів сеансу TLS і сеансу IPsec, показали, що IPsec вимагає приблизно в 20 разів (26 мс проти 1.3 мс) більше часу на зміну ключів, ніж TLS. Це не великий період для одиничної зміни, але це може стати проблемою, якщо тисячі кінцевих пристроїв спробують змінити ключі одночасно.

Останнє питання - це затримка, пов'язана з відновленням безпечного з'єднання. SIP з використанням TLS вимагає мінімум 6 обмінів повідомленнями. Відновлення з'єднання SIP з використанням IPsec в основному пов'язано з виконанням протоколу IKE (Internet Key Exchange) і буде залежати від того як режим, основною, базовий або агресивний, використовується в першій фазі обміну. Вважаючи, що використовується основний режим, IPsec вимагає 9 обмінів повідомленнями (прим. Перекл. - в оригіналі мова йде про IKEv1 який, зараз заміщений IKEv2, а IKEv2, в свою чергу, вимагає 4 обміну, якщо не використовується EAP).

7. Управління мережею

Головною перевагою SRTP над IPsec є те, що заголовки UDP і RTP пакетів відкриті для персоналу обслуговування мережі, вони можуть використовувати отриману інформацію для пошуку та усунення мережевих

проблем. IPsec зашифровує ці заголовки, знищує таку інформацію З цієї ж точки зору, IPsec і TLS можна порівняти.

8. Приховування топології

IPsec має перевагу перед TLS і SRTP в плані приховування топології мережі, оскільки IPsec здатний инкапсулировать вихідний заголовок всередині зашифрованою навантаження, коли він використовується в тунельному режимі. TLS і SRTP не мають подібного функціоналу, і для його забезпечення повинні покладатися на зовнішнє NAT-пристрій. Однак, більшість реалізацій передачі даних використовуються не в тунельному, а в транспортному режимі, який так само не надає такого функціоналу.

Висновок: На підставі попереднього порівняння використання IPsec і зв'язки TLS + SRTP для захисту, рекомендується, що б розробники використовували TLS і SRTP. Такий підхід простіше впровадити і підтримувати, так само він більш вигідний, ніж IPsec, з точки зору використання смуги пропускання. Істотної переваги в безпеці від використання IPsec, в порівнянні з TLS і SRTP, немає. Такі висновки ґрунтуються на аналізі існуючих стандартів, поточних реалізацій TLS і SRTP у постачальників і науково-орієнтованих реалізацій IPsec, а так само на раніше опублікованих порівняннях. Однак, опублікованих робіт, в яких порівнюються реалізації IPsec і TLS / SRTP для забезпечення безпеки сеансів голосового зв'язку в робочих умовах або не існує, або вони обмежені і пропонують лише грунт для подальших використань. Однією з цілей подальших досліджень можуть стати ефективні механізми передачі ключової інформації IPsec через SIP повідомлення і порівняння безпеки і продуктивності для кожного підходу.

2.4 Автентифікація в протоколах IPSec

Структура IPSec була описана в попередніх розділах. В цьому ж пункті давайте розглянемо IPSec з точки зору забезпечення автентифікації

Протокол IPsec дозволяє транспортувати будь-який IP-трафік через VPN незалежно від того, який протокол більш високого рівня використовує трафік поверх протоколу IP.

Хости можуть здійснювати зв'язок через VPN-протокол IPsec, як якщо б це було нормальне посилання без необхідності конфігурацій, специфічних для програми, на шлюзовому пристрої. IPsec є частиною стандартів IPv4 і IPv6. IPsec визначений у RFC 4301.[21]

Коли трафік передається через VPN IPsec, шлюз або клієнт VPN на джерелі зв'язку контактує з шлюзом у пункті зв'язку, щоб встановити тунель VPN. Оригінальні пакети інкапсулюються, коли вони входять до тунелю, і де-інкапсулюються, коли вони виходять з тунелю в пункт призначення. Між тим, у трафіку можуть бути виявлені тільки зашифровані пакети. Хости, які здійснюють зв'язок через тунель, не знають про VPN. Комунікації передаються через тунель, як якщо б два шлюзи були з'єднані безпосередньо один з одним.

Тунельні та транспортні режими:

1. Режим тунелю інкапсулює повний оригінальний пакет у новий пакет IPsec і призначений для VPN-сайтів від сайту до сайту та мобільних VPN. Тунелі IPsec у VPN на основі політики завжди використовують режим тунелю. Тунелі в VPN на основі маршрутів можуть використовувати тунельний режим.
2. Режим транспортування не інкапсулює пакети в нові пакети IPsec. Замість цього, для інкапсуляції тунельованого трафіку використовується інкапсуляція, наприклад загальна інкапсуляція маршрутизації (GRE) або IP в IP (IP-IP). Тунелі в VPN на основі маршрутів можуть використовувати транспортний режим.

Асоціації безпеки (SA) в IPSec VPN

Параметри, які використовуються для тунелю, зберігаються в

асоціаціях безпеки (SA). Для кожного IPsec VPN-тунелю є два SA: один для вихідного трафіку та інший для вхідного трафіку.

Для того, щоб будь-які комунікації могли використовувати VPN, шлюзи повинні будувати і підтримувати тунелі VPN. Шлюзи обговорюють, які параметри використовувати між собою. Шлюзи зберігають цю інформацію таким чином, щоб її можна було використовувати для обробки трафіку протягом усього терміну життя тунелю VPN.

Термін SPI (індекс параметрів безпеки) іноді використовується з SA в VPN VPN. SPI використовуються для ідентифікації SA.

З міркувань безпеки кожен SA має час закінчення терміну дії. Після закінчення терміну дії шлюзи відкидають старі SA і погоджуються з новими, якщо все ще трафік проходить через VPN.

Заголовок автентифікації (AH) і інкапсуляція корисного навантаження безпеки (ESP) в VPN

Після встановлення IPsec VPN-тунелю будь-який трафік, що проходить через тунель, надсилається або у вигляді заголовка автентифікації (AH) або пакетів інкапсуляції безпеки (ESP).

1. Протокол IPsec AH не забезпечує шифрування даних, тому звичайний AH не призводить до VPN у повному значенні слова. Будь-хто, хто може перехопити транзитні пакети, може переглядати передані дані. AH може використовуватися для забезпечення автентифікації та цілісності даних у зв'язку, які не потребують шифрування.

   Рідко виникає потреба в застосуванні лише АГ. Тільки AH може використовуватися, коли для даних не потрібно шифрування, але ESP з шифруванням Null також може використовуватися для досягнення тієї ж мети.
2. Протокол IPsec ESP забезпечує автентифікацію, шифрування та перевірку цілісності, забезпечуючи безпечну передачу даних. Цей протокол є тим, що зазвичай мається на увазі під терміном VPN,

оскільки передані дані приховані від сторонніх. Як загальне орієнтир, використовуйте ESP для будь-якого нормального тунелювання VPN (дані, інкапсульовані в корисному навантаженні ESP).

3. Стандарти IPsec також підтримують комбінацію ESP і AH. Однак, цей варіант не забезпечує значного поліпшення безпеки типу VPN.

Перевірка автентичності підтверджує, що віддалена сторона є тим, кого вони стверджують (наприклад, щоб запобігти атаці з людиною в середині). Стандарт IPsec передбачає підтримку деяких опцій, але також дозволяє іншим опціям, що забезпечуються IPsec-сумісними продуктами бути ввімкненими. RFC 4305 перелічує стандартні вимоги IPsec, які повинні виконувати всі IPsec-сумісні продукти.

Спільний ключ (Shared Key) - це набір символів, який використовується як ключ автентифікації. Ви можете використовувати попередньо розділені ключі для автентифікації VPN зсередини сайту і з клієнтами VPN третіх сторін.

Обидва шлюзи створюють хеш-значення на основі попередньо спільного ключа та іншої інформації. Хеш-значення потім обмінюються і перевіряються для автентифікації іншої сторони. Як випливає з назви, попередньо розділений ключ повинен бути заздалегідь поширений на всі пристрої, які його використовують. Попередньо поділені ключі повинні бути передані конфіденційно, оскільки їх переваги безпеки негайно втрачаються, якщо ключ піддається неавторизованим сторонам.

Ключі попереднього спільного доступу також повинні бути довгими і випадковими, щоб бути безпечними. Короткі або передбачувані попередньо поділені ключі можуть бути легко розбиті в атаках з використанням грубої сили. Адміністратори також повинні пам'ятати, що періодично оновлювати попередньо спільні ключі для підтримки високого рівня безпеки. Stonesoft NGFW містить інструменти для генерації досить

довгих, випадкових попередньо розділених ключів для компонентів VPN. Клавіші автоматично передаються на будь-які двигуни Stonesoft NGFW, які потребують їх, використовуючи захищений канал зв'язку системи.

Також слід розглянути автентифікацію на основі сертифікатів. У всіх VPN-мережах від сайту до сайту та у мобільних VPN з клієнтами сторонніх VPN можна вибрати, чи використовувати сертифікати або спільний ключ для автентифікації. За допомогою клієнта Stonesoft VPN доступні такі типи автентифікації:

1. Гібридна автентифікація вимагає наявності дійсного сертифіката на шлюзі і деякої іншої форми автентифікації від користувача клієнта VPN.
2. Для автентифікації обміну сертифікатами необхідний сертифікат як від шлюзу, так і від клієнта VPN.

Сертифікати часто забезпечують кращу реальну безпеку, ніж спільні ключі. Сертифікати потрібно поновлювати лише з інтервалом у кілька років і мати механізм автоматичного закінчення терміну дії, який гарантує поновлення сертифіката. Файли сертифікатів не можуть бути скомпрометовані під час транзиту, оскільки вони не можуть бути використані без приватного ключа шифрування. Наведена нижче ілюстрація (Рис. 2.7.)описує основи створення сертифіката.

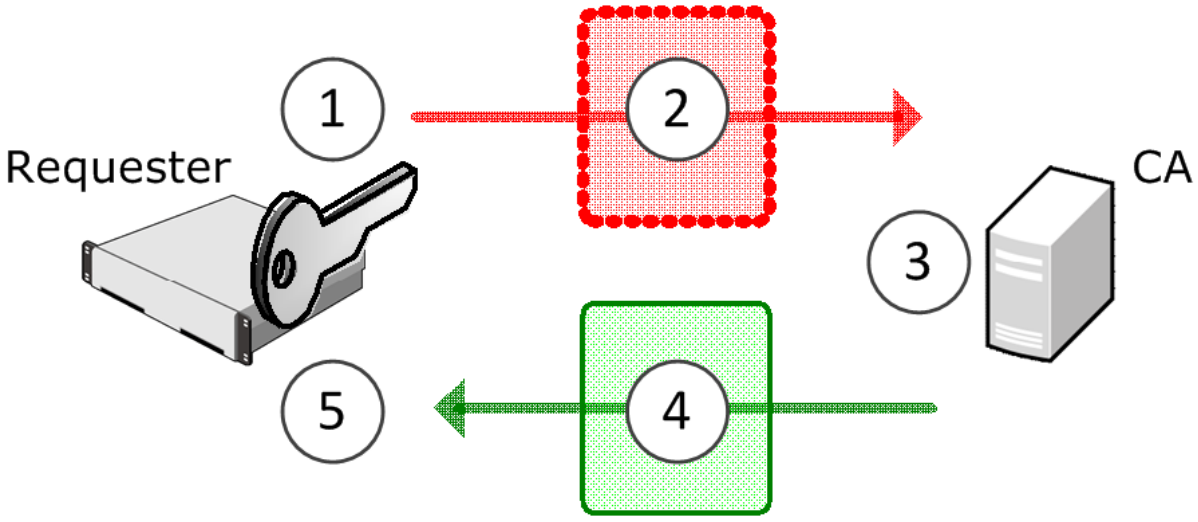

Рисунок 2.5 - Створення сертифікату VPN [21]

Після створення сертифікатів виконуються такі дії:

1. При запуску процесу запиту сертифіката генерується і зберігається приватний ключ шифрування.
2. Запитник сертифікатів використовує закритий ключ для створення зашифрованого запиту сертифіката, який передається до центру сертифікації (CA).
3. CA підписує зашифрований запит сертифіката, який перевіряє сертифікат.
4. Підписаний сертифікат передається оригінальному запитувачу сертифікату.
5. Запитувач використовує свій збережений закритий ключ для доступу до сертифіката.

Створення сертифіката може відбуватися або автоматично, або вручну:

1. Для шлюзів VPN всі кроки можуть бути автоматичними, якщо для підписання сертифіката використовується внутрішній сертифікат. Якщо використовується інший орган сертифікації, запит сертифіката експортується з SMC і підписаний сертифікат імпортується назад до SMC як файл.
2. Для клієнтів VPN файл запиту на сертифікат створюється вручну в клієнті VPN і передається вручну для підписання внутрішнім центром сертифікації або іншим центром сертифікації. Підписаний сертифікат потім передається вручну в клієнтський комп'ютер VPN.

Приватні ключі завжди створюються автоматично. Якщо закритий ключ втрачено (наприклад, через збій обладнання), будь-який асоційований сертифікат стає непридатним для використання, а новий сертифікат

повинен бути створений. Приватний ключ надійно і автоматично синхронізується між кластерними вузлами брандмауера, щоб всі вузли могли використовувати один і той же сертифікат.

На відміну від попередньо поділених ключів, сертифікати не повинні поширюватися на всі шлюзи VPN. Замість цього інші шлюзи налаштовані на довіру до емітента сертифіката (ЦС, який підписав сертифікат), після чого вони довіряють всім сертифікатам цього емітента. Цей довірчий зв'язок також дозволяє поновлювати або повторно створювати сертифікат на одному шлюзі без необхідності перенастроювати інші шлюзи. Тільки сертифікати з надійних джерел приймаються під час автентифікації. З цієї причини шлюзи VPN повинні бути налаштовані так, щоб довіряти органам сертифікації, які підписують сертифікати, які використовують інші шлюзи для автентифікації.

Сертифікати завжди діють, починаючи з певної дати та часу, і закінчуються на певну дату та час у майбутньому.

Усі компоненти, які використовують (або підписують) сертифікати, повинні мати правильні налаштування часу, щоб уникнути несподіваних відмов у видачі сертифіката. Внутрішній CA RS для шлюзів і внутрішній CA CA для шлюзів сервера керування генерують сертифікати, які дійсно починаються відразу до трьох років з моменту їх створення.

Списки відкликання сертифікатів (CRL) можна використовувати для скасування сертифіката, перш ніж вони закінчаться. Наприклад, сертифікат може бути анульований, якщо сторони, що не мають дозволу, отримали копію сертифіката та відповідного закритого ключа. Внутрішній CA RSA для шлюзів і внутрішній CA CA для шлюзів не підтримують списки відкликання сертифікатів. Якщо ви хочете використовувати CRL, ви повинні використовувати зовнішній центр сертифікації (або той, кого ви підтримуєте, або комерційну службу). Доступ до серверів CRL здійснюється за допомогою LDAP або HTTP (залежно від того, що вказує

сертифікат). Якщо всі визначені сервери CRL недоступні, сертифікати вважаються недійсними, доки CRL не можна перевірити. Можна налаштувати движок Stonesoft NGFW для прямого доступу до серверів CRL або використання протоколу OCSP.

Зовнішні органи сертифікації можуть створювати сертифікати для шлюзів VPN, зовнішніх шлюзів VPN або клієнтів VPN.

Усі сертифікати IPsec відповідають стандарту ITU-T X.509, який також використовується в протоколах, таких як TLS / SSL і HTTPS. Зовнішні органи сертифікації особливо корисні при створенні VPN з партнерськими організаціями. Використання зовнішніх сертифікатів дозволяє обом організаціям використовувати власний центр сертифікації. Різні шлюзи в VPN можуть мати сертифікати, підписані різними органами сертифікації.[22]

Для того, щоб двигуни Stonesoft NGFW приймали зовнішні підписані сертифікати зовнішніх компонентів, ви просто імпортуєте відкритий ключ зовнішнього сертифікату в SMC.

Наприклад, щоб створити сертифікат для двигунів Stonesoft NGFW або клієнта Stonesoft VPN, необхідно створити запит на сертифікат і надати йому підпис зовнішнього сертифікату. Зовнішній центр сертифікації повинен підтримувати запити сертифікатів PKCS # 10 у форматі PEM, а підписані сертифікати також повинні бути у форматі PEM. Крім того, центр сертифікації повинен мати можливість копіювати всі атрибути з запиту сертифіката в сертифікат. Зокрема, X.509 розширення Тема Альтернативна назва повинна бути скопійована в сертифікат, тому що його значення використовується для ідентифікації.

Висновки до розділу 2

В даному розіділі мною було розглянуті дві основні фундаментальні концепції, що є надзвичайно важливими в контексті розгляді проблеми

автентифікації в інтернеті речей - моедлі загроз в IoT та використання IPSec в IoT. Також було наведено приклади реалізованих методів автентифікації для різних потреб.

Головним висновком даного розділу варто відзначити те, що будь-якій системі автентифікації в IoT необхідно використовувати автентифікаційні можливості IPSec, як фундамент в побудові лінії захисту мережі.

3 ПОБУДОВА МЕТОДУ ОЦІНКИ ЕФЕКТИВНОСТІ ЗАСОБІВ АВТЕНТИФІКАЦІЇ

3.1 Підготовка моделі загроз

Згідно з головною метою даної роботи потрібно провести аналіз протоколів автентифікації для мереж інтернету речей. Так як більшість протоколів для реалізації потребують надзвичайно багато ресурсів для реалізації (наприклад, автентифікація користувача розумного будинку по індивідуальним особливостям ходи) пропоную розробити математичний апарат для метааналізу зібраних даних про протоколи автентифікації.

В другому розділі я будував загальну модель загроз для мереж інтернету речей. На даному етапі, після вивчення інформаційних ресурсів, джерел, прикладів реалізації протоколів автентифікації, специфікацій, матеріалів з конференцій, дисертацій та інших наукових робіт я пропоную більш конкретну модель загро, а саме зосередитися на п'яти атаках, які в основному становлять загрозу предметній області та вирішення яких пропонують нові протоколи автентифікації. Мною будуть враховані такі види основних атак:

1. MITM (man in the middle) людина-в-середині
2. Атака підміни ролі (impersonation attack)
3. Атака повторного відтворення (replay attack)

4. Атака вбудовування (forging attack)
5. Атаки Сибілли (Sybil attack)

Розглянемо більш конкретно кожен з видів атак.

Людина-в-середині (MITM) атака є однією з найбільш відомих нападів в IoT. З MITM атакою, зловмисник може обманювати ідентичності двох вузлів (нехай N1 і N2), що беруть участь у мережевому обміні і передають N1 для N2 і навпаки, тобто приймають контроль каналу зв'язку між N1 і N2. Маючи контроль цього каналу, зловмисник може перехопити, змінити, змінити, або замінити трафік комунікацій жертв.

Атака підміни ролі (impersonation attack) та атака вбудовування (forging attack) Під імітацією і втілюючи атаку в IoS, противник може підслуховувати або перехоплювати повідомлення про запит на вхід до попереднього під час виконання протоколу автентифікації. Після цього він може модифікувати і повторно передавати повідомлення для користувача, щоб видати себе як дійсний користувач мережі.

Атака повторного відтворення (replay attack) здійснюється на основі записаних раніше успішно відправлених повідомлень від автентифікованого користувача. В більшості випадків це такі дані, як паролі, логіни, файли сесій, біометричні дані

Атака Сибілли (Sybil attack) здійснюється в одноранговій мережі і в результаті точка доступу жертви підключається виключно до вузлів, що їх контролює зловмисник

Також будуть розглянуті менш небезпечні або ж рідкісні атаки

1. Атака зміни відстані (Changing distance attack)
2. Атака через пристрій того ж типу (Same-type-device attack)
3. Композиційна атака(Composition attack)
4. Атака перенаправлення(Redirection attack)
5. Атака заміни(Substitution attack)
6. Атака на відмову в обслуговуванні (DoS attack)

7. Атака впровадження вузлів (Colluding attack)
8. Атака перенаповненням (Flooding attack)
9. Атака стороннього каналу (Side-channel attack)
10. Атака фальшивим повідомленням (False messages attack)
11. Атака аудіоповторення (Audio replay attack)
12. Зміна повідомлення (Message modification)
13. Відстежування пересування (Movement tracking)
14. Атака вгадуванням (Guessing attack)
15. Атака вкраденим верифікатором (Stolen-verifier attack)
16. Атака на червоточину (Wormhole attack)
17. Атака чорної діри (Blackhole attack)
18. Атака відстежування атрибуту (Attribute-trace attack)
19. Підслуховування (Eavesdropping attack)
20. Атака обраного тексту (Chosen-plaintext attack)
21. Спам (Spam attack)
22. Атака викраденням ідентичності (Identity theft attack)
23. Маніпуляція користувачем (User manipulation attack)
24. Атака маршрутизації (Routing attack)
25. Атака зв’язності (Linkability attack)
26. Атака відмови (Rejection attack)
27. Атака вдалої відповіді (Successive-response attack)
28. Аналіз пакетів (Packet analysis attack)
29. Відстежування акетів (Packet tracing attack)
30. Атака перебором (Brute-force attack)

Всі атаки будуть класифіковані по 4-ом типам:

1. Тип A: пасивна або активна
2. Тип B: внутрішня чи зовнішня
3. Тип C: Атаки на основі ключів, атаки на основі даних, атаки на основі

уособлення та на основі фізичних даних атаки;

4. Тип D: Атаки на основі ідентичності, засновані на розташуванні атаки, атак основані на підслуховуванні, маніпулювання і атаки на основі служб

Також будуть враховуватися такі фактори, як наявність криптосистем і контрзаходів, плюси та мінуси кожної з реалізацій та відповідність складності реалізації до цілей.

3.2 Розробка методу оцінювання засобів автентифікації

Для вибору пріорітетних протоколів буде побудовано три матриці.

Матриця номер один - наявність захисту від певного виду атаки для кожного протоколу

Матриця номер два - наявність або ж відсутність криптосистем та контрзаходів.

Матриця номер три - мінуси та плюси кожної реалізації.

Оцінювання результатів перших двох матриць буде побудавно на основі математичного апарату, а матриці номер три - на основі конкретних потреб.

Для обрахування ефективності захисту від конкретних загроз буде використана формула:

$$\lambda = n - \sum_1^n k_i q_i \quad (3.1)$$

де λ - оцінка захищеності конкретного протоколу, n - к-ть досліджуваних атак, k - коефіцієнт впливу атаки, q - абсолютна оцінка захищеності від атаки (1 - захист є, 0 - захист нестабільний, -1 - захисту немає).

Матриця номер два представляє собою предикатну таблицю відповідності наявності певних криптографічних механізмів та методів контрзахисту, а саме:

1. Безпечні крипоткрафічні хеш-функції)Secure cryptographic hash function)

2. HORS схема (HORS scheme)
3. Heavy signing light verification
4. Light signing heavy verification
5. Merkle Hash tree technique
6. Короткі підписи (Short signatures (BLS))
7. Пакетна перевірка (Batch verification)
8. Агрегація підписів (Signature aggregation)
9. Криптосистема, що базується на ідентичності публічного ключа (Identity-based public key cryptosystem)
10. Шифрування публічним ключем (Public-key encryption, such as RSA)
11. HMAC, such as SHA-1 and MD5
12. Протокол встановлення ключа Діффі-Хеллмана (Diffie-Hellman key establishment protocol)
13. Механізм EIBC (EIBC mechanism)
14. ID-based cryptography (IBC)
15. Digital signatures
16. Homomorphic encryption
17. Bloom filter
18. Commitment scheme
19. Алгоритми симетричого шифрування/ розишфрування (Symmetric encryption/decryption algorithm)

Обчислення оцінки буде здійснене за формулою:

$$\alpha = \sum_1^n j_i \; l_i \tag{3.2}$$

де α - оцінка криптографічних методів та засобів контрзаходів, n - к-ть досліджуваних методів, j - коефіцієнт важливості, l - предикат наявності

Результуюча оцінка буде обрахована за наступною формулою:

$$\phi = \frac{\left(\frac{\alpha}{(m*2)}*\mu*\left(\frac{\lambda}{n}\right)*\upsilon*\Theta\right)}{\left(\frac{b}{a}\right)} \quad (3.3)$$

де ϕ - фінальна оцінка протоколу, μ - коефіцієнт критичності захищеності від атак, m - к-ть розглянутих атак, n- к-ть розглянутих методів криптографії та контрзаходів, υ- коефіцієнт критичності наявності криптографічних систем, b - к-ть врахованих плюсів a - к-ть врахованих мінусів. $\left(\frac{b}{a}\right)$ - є фактором суб'єктивності розглянутого протоколу коефіцієнт, Θ- врівноваження рівний 50. Для уникнення людського фактору раджу брати це відношення за 1. Обов'язковою умовою є μ+ υ= 10

3.3 Результати оцінки методів автентифікації в IoT

В даному підрозділі будуть сформовані матриці, що описувались в 3.2 та застосований розроблений мною математичний апарат для проведення порівняння протоколів автентифікації. В нижче наведених таблицях [n] означає протокол описаний в статті, що зсилається на джерело під номером n. Так зроблено через те, що таблиці стають занадто габаритними, якщо писати назви протоколів повністю. В побудованій нижче моделі коефіцієнти впливу та важливості вибрані довільно, щоб показати працездатність, а саме: коефіцієнт важливості наявності захисних механізмів від певних видів атак був обраний як 3, а коефіцієнт важливості наявності крпитографічних методів як 7

Коефіцієнти для кожного з видів атак відображені нижче:

Таблиця 3.1 - Розподілення коефіцієнтів важливості для видів атак

0,2	Audio replay attack
0,4	Changing distance attack
0,9	Same-type-device attack
0,2	Composition attack
0,8	Redirection attack
1	Man-in-the-middle attack
0,3	Substitution attack
0,5	DoS attack
1	Replay attack
1	Forging attack
0,9	Colluding attack
0,2	Flooding attack
0,4	Side-channel attack
0,4	False messages attack
1	Sybil attack
0,2	Movement tracking
0,1	Message modification
0,1	Impersonation attack
0,4	Guessing attack
0,2	Stolen-verifier attack
0,7	Wormhole attack
0,9	Blackhole attack
0,9	Attribute-trace attack
0,5	Eavesdropping attack
0,3	Chosen-plaintext attack
1	Spam attack
0,9	Identity theft attack
0,4	User manipulation attack
0,7	Routing attack
0,7	Linkability attack
0,1	Rejection attack
0,3	Successive-response attack
0,8	Packet analysis attack
0,1	Packet tracing attack
1	Brute-force attack

Таблиця 3.2 - Розподілення коефіцієнтів важливості для наявності криптосистем

Криптосистеми	j
Secure cryptographic hash function	1
Original data acquisition	0,6
Spatial-Domain transformation	0,3
Time-domain transformation	0,1
Correlation coefficient-based matching algorithm (C-MA)	0,8
Deviation ratio-based matching algorithm (D-MA)	0,6
Aggregate message authentication codes (AMACs)	0,4
Certificateless aggregate signature	0,5
Elliptic Curve Diffie-Hellman (ECDH)	0,4
ID-based signature scheme	0,5
Advanced encryption standard (AES)	0,2
Hybrid Linear Combination Encryption	0,5

Під час результуючого аналізу було розглянуто 36 різних методів автентифікації і для кожного була виведена остаточна оцінка на основі запропонованого мною аналітичного методу. Результати наведені нижче

Таблиця 3.3 - Оцінка захищеності від атак (частина перша)

		[62]		[61]		[46]		[38]		[34]		[53]		[47]		[137]		[37]	
Загроза	k	A	B	A	B	A	B	A	B	A	B	A	B	A	B	A	B	A	B
Audio replay attack	0,2	1	0,2	0	0	-1	-0,2	0	0	0	0	0	0	-1	-0,2	-1	-0,2	0	0
Changing distance attack	0,4	1	0,4	-1	-0,4	-1	-0,4	-1	-0,4	-1	-0,4	-1	-0,4	-1	-0,4	-1	-0,4	-1	-0,4
Same-type-device attack	0,9	1	0,9	-1	-0,9	-1	-0,9	-1	-0,9	-1	-0,9	-1	-0,9	-1	-0,9	-1	-0,9	-1	-0,9
Composition attack	0,2	1	0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2
Redirection attack	0,8	0	0	1	0	0	0	1	0,8	-1	-0,8	-1	-0,8	0	0	-1	-0,8	1	0,8
Man-in-the-middle attack	1	0	0	1	0	0	0	1	1	0	0	0	0	-1	-1	-1	-1	1	1
Substitution attack	0,3	0	0	0	0	0	0	0	0	0	0	-1	-0,3	-1	-0,3	-1	-0,3	-1	-0,3
DoS attack	0,5	-1	-0,5	1	-0,5	-1	-0,5	1	0,5	-1	-0,5	-1	-0,5	1	0,5	-1	-0,5	-1	-0,5
Replay attack	1	0	0	-1	-1	-1	-1	1	1	0	0	1	1	-1	-1	-1	-1	1	1
Forging attack	1	0	0	-1	-1	-1	-1	0	0	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1
Colluding attack	0,9	0	0	-1	-0,9	-1	-0,9	0	0	-1	-0,9	-1	-0,9	0	0	-1	-0,9	-1	-0,9
Flooding attack	0,2	0	0	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2	0	0	-1	-0,2	0	0
Side-channel attack	0,4	0	0	-1	-0,4	-1	-0,4	-1	-0,4	-1	-0,4	-1	-0,4	0	0	-1	-0,4	0	0
False messages attack	0,4	-1	-0,4	-1	-0,4	-1	-0,4	-1	-0,4	0	0	0	0	0	0	-1	-0,4	0	0
Sybil attack	1	-1	-1	-1	-1	-1	-1	-1	-1	0	0	0	0	-1	-1	-1	-1	0	0
Movement tracking	0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2	0	0	-1	-0,2	-1	-0,2	-1	-0,2	0	0
Message modification	0,1	-1	-0,1	-1	-0,1	-1	-0,1	-1	-0,1	0	0	-1	-0,1	-1	-0,1	-1	-0,1	-1	-0,1
Impersonation attack	0,1	-1	-0,1	-1	-0,1	-1	-0,1	-1	-0,1	0	0	1	0,1	1	0,1	-1	-0,1	-1	-0,1
Guessing attack	0,4	-1	-0,4	-1	-0,4	-1	-0,4	-1	-0,4	-1	-0,4	1	0,4	-1	-0,4	-1	-0,4	-1	-0,4
Stolen-verifier attack	0,2	0	0	0	-0,2	-1	-0,2	-1	-0,2	-1	-0,2	1	0,2	-1	-0,2	-1	-0,2	-1	-0,2
Wormhole attack	0,7	0	0	0	-0,7	-1	-0,7	0	0	-1	-0,7	0	0	-1	-0,7	-1	-0,7	0	0
Blackhole attack	0,9	0	0	-1	-0,9	-1	-0,9	0	0	0	0	0	0	-1	-0,9	-1	-0,9	0	0
Attribute-trace attack	0,9	-1	-0,9	-1	-0,9	-1	-0,9	-1	-0,9	0	0	-1	-0,9	-1	-0,9	-1	-0,9	-1	-0,9
Eavesdropping attack	0,5	-1	-0,5	-1	-0,5	-1	-0,5	-1	-0,5	0	0	0	0	-1	-0,5	-1	-0,5	0	0
Chosen-plaintext attack	0,3	-1	-0,3	-1	-0,3	-1	-0,3	-1	-0,3	0	0	-1	-0,3	-1	-0,3	-1	-0,3	0	0
Spam attack	1	0	0	-1	-1	-1	-1	-1	-1	0	0	0	0	-1	-1	-1	-1	0	0
Identity theft attack	0,9	0	0	-1	-0,9	-1	-0,9	-1	-0,9	-1	-0,9	0	0	-1	-0,9	-1	-0,9	-1	-0,9
User manipulation attack	0,4	0	0	-1	-0,4	-1	-0,4	-1	-0,4	-1	-0,4	0	0	0	0	-1	-0,4	0	0
Routing attack	0,7	0	0	-1	-0,7	-1	-0,7	-1	-0,7	-1	-0,7	0	0	-1	-0,7	-1	-0,7	-1	-0,7
Linkability attack	0,7	0	0	-1	-0,7	-1	-0,7	-1	-0,7	-1	-0,7	-1	-0,7	-1	-0,7	-1	-0,7	-1	-0,7
Rejection attack	0,1	-1	-0,1	-1	-0,1	-1	-0,1	-1	-0,1	-1	-0,1	-1	-0,1	-1	-0,1	-1	-0,1	-1	-0,1
Successive-response attack	0,3	-1	-0,3	-1	-0,3	-1	-0,3	-1	-0,3	-1	-0,3	-1	-0,3	-1	-0,3	-1	-0,3	-1	-0,3
Packet analysis attack	0,8	-1	-0,8	0	-0,8	-1	-0,8	-1	-0,8	-1	-0,8	0	0	-1	-0,8	-1	-0,8	0	0
Packet tracing attack	0,1	-1	-0,1	0	-0,1	-1	-0,1	-1	-0,1	-1	-0,1	0	0	-1	-0,1	-1	-0,1	0	0
Brute-force attack	1	0	0	0	-1	-1	-1	0	0	0	0	-1	-1	0	0	0	0	-1	-1
			31		17,4		17,6		27,1		24,4		27,5		20,8		16,5		28,2

Таблиця 3.4 - Оцінка захищеності від атак (частина друга)

		[39]		[40]		[63]		[64]		[65]		[66]		[48]		[52]		[54]	
Загроза	k	A	B	A	B	A	B	A	B	A	B	A	B	A	B	A	B	A	B
Audio replay attack	0,2	0	0	0	0	0	0	-1	-0,2	0	0	0	0	-1	-0,2	-1	-0,2	-1	-0,2
Changing distance attack	0,4	-1	-0,4	-1	-0,4	-1	-0,4	-1	-0,4	-1	-0,4	-1	-0,4	-1	-0,4	-1	-0,4	-1	-0,4
Same-type-device attack	0,9	-1	-0,9	-1	-0,9	-1	-0,9	-1	-0,9	-1	-0,9	-1	-0,9	-1	-0,9	-1	-0,9	-1	-0,9
Composition attack	0,2	0	0	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2
Redirection attack	0,8	1	0,8	0	-0,8	-1	-0,8	-1	-0,8	-1	-0,8	-1	-0,8	-1	-0,8	-1	-0,8	-1	-0,8
Man-in-the-middle attack	1	0	0	0	0	0	0	-1	-1	-1	-1	1	1	0	0	-1	-1	-1	-1
Substitution attack	0,3	1	0,3	0	0	0	0	-1	-0,3	-1	-0,3	0	0	1	0,3	-1	-0,3	-1	-0,3
DoS attack	0,5	1	0,5	-1	-0,5	-1	-0,5	1	0,5	1	0,5	1	0,5	-1	-0,5	-1	-0,5	-1	-0,5
Replay attack	1	0	0	1	1	1	1	-1	-1	0	0	-1	-1	0	0	-1	-1	0	0
Forging attack	1	0	0	1	-1	-1	-1	-1	-1	-1	-1	-1	-1		0	-1	-1	-1	-1
Colluding attack	0,9	-1	-0,9	1	-0,9	-1	-0,9	0	0	-1	-0,9	-1	-0,9		0	-1	-0,9	-1	-0,9
Flooding attack	0,2	-1	-0,2	-1	-0,2	-1	-0,2	0	0	-1	-0,2	-1	-0,2		0	-1	-0,2	-1	-0,2
Side-channel attack	0,4	-1	-0,4	-1	-0,4	-1	-0,4	0	0	1	0,4	-1	-0,4		0	-1	-0,4	0	0
False messages attack	0,4	0	0	-1	-0,4	-1	-0,4	-1	-0,4	1	0,4	-1	-0,4		0	-1	-0,4	0	0
Sybil attack	1	-1	-1	-1	-1	-1	-1	-1	-1	1	1	0	0		0	-1	-1	-1	-1
Movement tracking	0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2		0	-1	-0,2	-1	-0,2
Message modification	0,1	-1	-0,1	-1	-0,1	-1	-0,1	-1	-0,1	-1	-0,1	-1	-0,1		0	-1	-0,1	-1	-0,1
Impersonation attack	0,1	-1	-0,1	-1	-0,1	-1	-0,1	-1	-0,1	-1	-0,1	-1	-0,1	0	0	-1	-0,1	0	0
Guessing attack	0,4	0	0	0	-0,4	-1	-0,4	-1	-0,4	0	0	1	0,4		0	-1	-0,4	0	0
Stolen-verifier attack	0,2	0	0	0	-0,2	-1	-0,2	-1	-0,2	0	0	-1	-0,2	0	0	-1	-0,2	0	0
Wormhole attack	0,7	-1	-0,7	-1	-0,7	-1	-0,7	-1	-0,7	-1	-0,7	0	0	0	0	-1	-0,7	0	0
Blackhole attack	0,9	-1	-0,9	-1	0	0	0	0	0	0	0	-1	-0,9		0	-1	-0,9	0	0
Attribute-trace attack	0,9	-1	-0,9	-1	-0,9	-1	-0,9	0	0	-1	-0,9	-1	-0,9		0	-1	-0,9	0	0
Eavesdropping attack	0,5	-1	-0,5	-1	-0,5	-1	-0,5	0	0	-1	-0,5	-1	-0,5		0	-1	-0,5	0	0
Chosen-plaintext attack	0,3	-1	-0,3	-1	-0,3	-1	-0,3	0	0	-1	-0,3	-1	-0,3		0	-1	-0,3	-1	-0,3
Spam attack	1	-1	-1	-1	-1	-1	-1	0	0	-1	-1	-1	-1		0	0	0	-1	-1
Identity theft attack	0,9	-1	-0,9	-1	-0,9	-1	-0,9	0	0	-1	-0,9	-1	-0,9		0	0	0	-1	-0,9
User manipulation attack	0,4	-1	-0,4	-1	-0,4	-1	-0,4	0	0	-1	-0,4	-1	-0,4		0	0	0	0	0
Routing attack	0,7	0	0	-1	0	0	0	-1	-0,7	0	0	-1	-0,7		0	0	0	-1	-0,7
Linkability attack	0,7	-1	-0,7	-1	-0,7	-1	-0,7	-1	-0,7	-1	-0,7	0	0		0	0	0	0	0
Rejection attack	0,1	-1	-0,1	-1	-0,1	-1	-0,1	-1	-0,1	-1	-0,1	0	0		0	-1	-0,1	-1	-0,1
Successive-response attack	0,3	-1	-0,3	-1	-0,3	-1	-0,3	-1	-0,3	-1	-0,3	0	0		0	-1	-0,3	0	0
Packet analysis attack	0,8	0	0	0	-0,8	-1	-0,8	-1	-0,8	0	0	0	0		0	-1	-0,8	0	0
Packet tracing attack	0,1	0	0	0	-0,1	-1	-0,1	-1	-0,1	0	0	0	0		0	-1	-0,1	0	0
Brute-force attack	1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	0	0		0	-1	-1	0	0
			24,7		20,		20,6		22,9		24,4		24,5		32,3		19,2		24,3

Таблиця 3.5 - Оцінка захищеності від атак (частина третя)

		[28]		[49]		[138]		[139]		[140]		[141]		[142]		[55]		[67]	
Загроза	k	A	B	A	B	A	B	A	B	A	B	A	B	A	B	A	B	A	B
Audio replay attack	0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2
Changing distance attack	0,4	0	0	-1	-0,4	-1	-0,4	-1	-0,4	-1	-0,4	0	0	0	0	0	0	-1	-0,4
Same-type-device attack	0,9	-1	-0,9	-1	-0,9	-1	-0,9	0	0	-1	-0,9	-1	-0,9	-1	-0,9	-1	-0,9	-1	-0,9
Composition attack	0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2
Redirection attack	0,8	-1	-0,8	-1	-0,8	-1	-0,8	0	0	-1	-0,8	0	0	-1	-0,8	-1	-0,8	-1	-0,8
Man-in-the-middle attack	1	0	0	-1	0	0	0	1	1	0	0	0	0	1	1	0	0	0	0
Substitution attack	0,3	-1	-0,3	0	-0,3	-1	-0,3	-1	-0,3	-1	-0,3	-1	-0,3	0	0	0	0	-1	-0,3
DoS attack	0,5	-1	-0,5	0	0	0	0	1	0,5	-1	-0,5	0	0	1	0,5	-1	-0,5	0	0
Replay attack	1	0	0	1	0	0	0	1	1	1	1	1	1	1	1	0	0	1	1
Forging attack	1	1	1	0	0	0	0	0	0	0	0	-1	-1	-1	-1	-1	-1	-1	-1
Colluding attack	0,9	-1	-0,9	0	-0,9	-1	-0,9	0	0	0	0	-1	-0,9	0	0	0	0	-1	-0,9
Flooding attack	0,2	-1	-0,2	0	-0,2	-1	-0,2	0	0	-1	-0,2	-1	-0,2	0	0	0	0	0	0
Side-channel attack	0,4	-1	-0,4	-1	-0,4	-1	-0,4	-1	-0,4	-1	-0,4	0	0	0	0	0	0	-1	-0,4
False messages attack	0,4	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0,4
Sybil attack	1	0	0	0	0	0	0	0	0	0	0	0	0	-1	-1	-1	-1	0	0
Movement tracking	0,2	0	0	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2	0	0	-1	-0,2	-1	-0,2	0	0
Message modification	0,1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0,1
Impersonation attack	0,1	0	0	0	-0,1	-1	-0,1	-1	-0,1	0	0	-1	-0,1	0	0	0	0	0	0
Guessing attack	0,4	-1	-0,4	0	-0,4	-1	-0,4	0	0	-1	-0,4	-1	-0,4	-1	-0,4	-1	-0,4	-1	-0,4
Stolen-verifier attack	0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2	0	0	-1	-0,2	-1	-0,2	-1	-0,2
Wormhole attack	0,7	-1	-0,7	-1	0	0	0	-1	-0,7	-1	-0,7	0	0	0	0	0	0	0	0
Blackhole attack	0,9	-1	-0,9	-1	0	0	0	0	0	-1	-0,9	0	0	0	0	0	0	0	0
Attribute-trace attack	0,9	-1	-0,9	-1	-0,9	-1	-0,9	0	0	0	0	0	0	-1	-0,9	-1	-0,9	-1	-0,9
Eavesdropping attack	0,5	0	0	0	0	0	0	0	0	-1	-0,5	1	0,5	0	0	0	0	0	0
Chosen-plaintext attack	0,3	-1	-0,3	-1	-0,3	-1	-0,3	0	0	-1	-0,3	-1	-0,3	-1	-0,3	-1	-0,3	-1	-0,3
Spam attack	1	-1	-1	-1	-1	-1	-1	0	0	0	0	-1	-1	-1	-1	-1	-1	-1	-1
Identity theft attack	0,9	-1	-0,9	-1	0	0	0	-1	-0,9	0	0	-1	-0,9	0	0	0	0	0	0
User manipulation attack	0,4	-1	-0,4	-1	-0,4	-1	-0,4	0	0	-1	-0,4	-1	-0,4	-1	-0,4	-1	-0,4	0	0
Routing attack	0,7	-1	-0,7	-1	0	0	0	0	0	-1	-0,7	-1	-0,7	-1	-0,7	-1	-0,7	-1	-0,7
Linkability attack	0,7	0	0	-1	0	0	0	0	0	-1	-0,7	-1	-0,7	0	0	0	0	-1	-0,7
Rejection attack	0,1	0	0	-1	0	0	0	0	0	0	0	-1	-0,1	0	0	0	0	0	0
Successive-response attack	0,3	0	0	-1	-0,3	-1	-0,3	0	0	-1	-0,3	-1	-0,3	-1	-0,3	-1	-0,3	0	0
Packet analysis attack	0,8	0	0	1	0	0	0	0	0	0	0	-1	-0,8	0	0	0	0	1	0,8
Packet tracing attack	0,1	0	0	0	-0,1	-1	-0,1	0	0	0	0	0	0	0	0	0	0	0	0
Brute-force attack	1	-1	-1	-1	-1	-1	-1	1	1	-1	-1	-1	-1	1	1	0	0	-1	-1
			24,2		25,2		25,8		34,9		25,8		26,1		30		26		27

Таблиця 3.6 - Оцінка захищеності від атак (частина четверта)

		[68]		[69]		[143]		[70]		[71]		[72]		[73]		[74]		[75]	
Загроза	k	A	B	A	B	A	B	A	B	A	B	A	B	A	B	A	B	A	B
Audio replay attack	0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2	-1	-0,2
Changing distance attack	0,4	0	0	-1	0	0	0	-1	-0,4	-1	-0,4	-1	-0,4	-1	-0,4	-1	-0,4	-1	-0,4
Same-type-device attack	0,9	0	0	-1	0	0	0	-1	-0,9	-1	-0,9	-1	-0,9	-1	-0,9	-1	-0,9	0	0
Composition attack	0,2	1	0,2	0	-0,2	-1	-0,2	-1	-0,2	0	0	0	0	-1	-0,2	0	0	0	0
Redirection attack	0,8	1	0,8	0	0	0	0	-1	-0,8	-1	-0,8	0	0	0	0	0	0	0	0
Man-in-the-middle attack	1	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	1	1
Substitution attack	0,3	0	0	-1	-0,3	-1	-0,3	0	0	-1	-0,3	-1	-0,3	0	0	-1	-0,3	0	0
DoS attack	0,5	0	0	0	0	0	0	-1	-0,5	0	0	-1	-0,5	0	0	-1	-0,5	1	0,5
Replay attack	1	1	1	0	1	1	1	1	1	0	0	1	1	1	1	0	0	1	1
Forging attack	1	0	0	1	0	0	0	-1	-1	0	0	1	1	0	0	0	0	0	0
Colluding attack	0,9	0	0	0	0	0	0	-1	-0,9	0	0	0	0	0	0	-1	-0,9	0	0
Flooding attack	0,2	1	0,2	0	-0,2	-1	-0,2	-1	-0,2	0	0	0	0	0	0	-1	-0,2	0	0
Side-channel attack	0,4	-1	-0,4	0	-0,4	-1	-0,4	-1	-0,4	-1	-0,4	-1	-0,4	-1	-0,4	-1	-0,4	-1	-0,4
False messages attack	0,4	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sybil attack	1	0	0	0	1	1	1	0	0	-1	-1	-1	-1	-1	-1	0	0	0	0
Movement tracking	0,2	0	0	0	-0,2	-1	-0,2	-1	-0,2	0	0	-1	-0,2	-1	-0,2	0	0	0	0
Message modification	0,1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0,1	0	0
Impersonation attack	0,1	1	0,1	1	0	0	0	1	0,1	1	0,1	0	0	0	0	1	0,1	0	0
Guessing attack	0,4	1	0,4	1	0	0	0	1	0,4	0	0	0	0	0	0	0	0	0	0
Stolen-verifier attack	0,2	1	0,2	-1	-0,2	-1	-0,2	0	0	0	0	-1	-0,2	-1	-0,2	-1	-0,2	1	0,2
Wormhole attack	0,7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	-0,7	-1	-0,7
Blackhole attack	0,9	0	0	0	0	0	0	0	0	-1	-0,9	0	0	0	0	-1	-0,9	-1	-0,9
Attribute-trace attack	0,9	-1	-0,9	-1	-0,9	-1	-0,9	-1	-0,9	0	0	0	0	-1	-0,9	-1	-0,9	0	0
Eavesdropping attack	0,5	0	0	0	0	0	0	0	0	-1	-0,5	0	0	0	0	-1	-0,5	0	0
Chosen-plaintext attack	0,3	-1	-0,3	-1	-0,3	-1	-0,3	-1	-0,3	0	0	-1	-0,3	-1	-0,3	-1	-0,3	-1	-0,3
Spam attack	1	-1	-1	-1	-1	-1	-1	0	0	-1	-1	-1	-1	0	0	-1	-1	0	0
Identity theft attack	0,9	0	0	0	0	0	0	-1	-0,9	-1	-0,9	-1	-0,9	0	0	-1	-0,9	0	0
User manipulation attack	0,4	0	0	0	-0,4	-1	-0,4	0	0	0	0	-1	-0,4	0	0	0	0	0	0
Routing attack	0,7	0	0	0	0	0	0	0	0	0	0	-1	-0,7	0	0	-1	-0,7	0	0
Linkability attack	0,7	0	0	0	0	0	0	0	0	0	0	-1	-0,7	0	0	-1	-0,7	0	0
Rejection attack	0,1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	-0,1	0	0
Successive-response attack	0,3	1	0,3	-1	0	0	0	-1	0	0	0	-1	-0,3	-1	-0,3	-1	-0,3	0	0
Packet analysis attack	0,8	0	0	0	-0,8	-1	-0,8	0	0	0	0	-1	-0,8	-1	-0,8	1	0,8	-1	-0,8
Packet tracing attack	0,1	0	0	0	-0,1	-1	-0,1	0	0	1	0,1	-1	-0,1	-1	-0,1	1	0,1	-1	-0,1
Brute-force attack	1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1
			34,4		30,		30,8		27,7		26,9		27,7		29,1		24,1		32,9

Таблиця 3.7 - Оцінка наявності криптографічних механізмів(частина перша)

Криптосистеми	j	62	61	46	38	34	53	47	137	37	39	40	63	64	65	66	48	52	54
Secure cryptographic hash function	1		1	1	1	1	1		1	1		1	1	1	1	1		1	1
Original data acquisition	0,6								0,6		0,6								
Spatial-Domain transformation	0,3								0,3		0,3								
Time-domain transformation	0,1								0,1			0,1							
Correlation coefficient-based matching algorithm (C-MA)	0,8	0,8											0,8						
Deviation ratio-based matching algorithm (D-MA)	0,6	0,6												0,6					
Aggregate message authentication codes (AMACs)	0,4		0,4							0,4				0,4				0,4	
Certificateless aggregate signature	0,5			0,5										0,5				0,5	
Elliptic Curve Diffie-Hellman (ECDH)	0,4				0,4										0,4				
ID-based signature scheme	0,5					0,5													0,5
Advanced encryption standard (AES)	0,2						0,2									0,2			
Hybrid Linear Combination Encryption	0,5							0,5									0,5		
		1,4	1,4	1,5	1,4	1,5	1,2	0,5	2	1,4	0,9	1,1	1,8	2,5	1,4	1,2	0,5	1,9	1,5

Таблиця 3.8 - Оцінка наявності криптографічних механізмів(частина друга)

Криптосистеми	j	28	49	138	139	140	141	142	55	67	68	69	143	70	71	72	73	74	75
Secure cryptographic hash function	1	1		1			1	1			1	1	1	1	1	1	1	1	1
Original data acquisition	0,6	0,6									0,6								
Spatial-Domain transformation	0,3	0,3									0,3								
Time-domain transformation	0,1	0,1										0,1		0,1	0,1				
Correlation coefficient-based matching algorithm (C-MA)	0,8		0,8										0,8						
Deviation ratio-based matching algorithm (D-MA)	0,6			0,6												0,6			
Aggregate message authentication codes (AMACs)	0,4			0,4												0,4			
Certificateless aggregate signature	0,5			0,5					0,5							0,5	0,5	0,5	0,5
Elliptic Curve Diffie-Hellman (ECDH)	0,4				0,4				0,4	0,4						0,4			
ID-based signature scheme	0,5					0,5											0,5	0,5	
Advanced encryption standard (AES)	0,2					0,2													
Hybrid Linear Combination Encryption	0,5								0,5	0,5						0,5			
		2	0,8	2,5	0,4	0,7	1	1	1,4	0,9	1,9	1,1	1,8	1,1	1,1	3,4	2	2	1,5

Нижче наведена результуюча таблиця з використанням побудованої моделі оцінювання:

Таблиця 3.9 - Таблиця з результатами оцінювання

	alpha	mu	m	sh	n	v	sigma	b	a	Res
[62]	31	3	35	1,4	12	7	50	1	1	54,2
[61]	17,8	3	35	1,4	12	7	50	1	1	31,1
[46]	17,6	3	35	1,5	12	7	50	1	1	33
[38]	27,1	3	35	1,4	12	7	50	1	1	47,4
[34]	24,4	3	35	1,5	12	7	50	1	1	45,7
[53]	27,5	3	35	1,2	12	7	50	1	1	41,2
[47]	20,8	3	35	0,5	12	7	50	1	1	13
[137]	16,5	3	35	2	12	7	50	1	1	41,2
[37]	28,2	3	35	1,4	12	7	50	1	1	49,3
[39]	24,7	3	35	0,9	12	7	50	1	1	27,7
[40]	20,6	3	35	1,1	12	7	50	1	1	28,3
[63]	20,6	3	35	1,8	12	7	50	1	1	46,3
[64]	22,9	3	35	2,5	12	7	50	1	1	71,5
[65]	24,4	3	35	1,4	12	7	50	1	1	42,7
[66]	24,5	3	35	1,2	12	7	50	1	1	36,7
[48]	32,3	3	35	0,5	12	7	50	1	1	20,1
[52]	19,2	3	35	1,9	12	7	50	1	1	45,6
[54]	24,3	3	35	1,5	12	7	50	1	1	45,5
[28]	24,2	3	35	2	12	7	50	1	1	60,5
[49]	25,8	3	35	0,8	12	7	50	1	1	25,8
[138]	25,8	3	35	2,5	12	7	50	1	1	80,6
[139]	34,9	3	35	0,4	12	7	50	1	1	17,4
[140]	25,8	3	35	0,7	12	7	50	1	1	22,5
[141]	26,1	3	35	1	12	7	50	1	1	32,6
[142]	30	3	35	1	12	7	50	1	1	37,5
[55]	26	3	35	1,4	12	7	50	1	1	45,5
[67]	27	3	35	0,9	12	7	50	1	1	30,3
[68]	34,4	3	35	1,9	12	7	50	1	1	81,7
[69]	30,8	3	35	1,1	12	7	50	1	1	42,3
[143]	30,8	3	35	1,8	12	7	50	1	1	69,3
[70]	27,7	3	35	1,1	12	7	50	1	1	38,0
[71]	26,9	3	35	1,1	12	7	50	1	1	36,9
[72]	27,7	3	35	3,4	12	7	50	1	1	117,
[73]	29,1	3	35	2	12	7	50	1	1	72,7
[74]	24,1	3	35	2	12	7	50	1	1	60,2
[75]	32,9	3	35	1,5	12	7	50	1	1	61,6

Всі результати обрахування доступні за посиланням

https://docs.google.com/spreadsheets/d/11R5aLhUmx2U4hEpZ9n3QVQAaYwZNrA3Px9rXpUjzhqw/edit#gid=0 (потрібно запрошувати доступ)

Тепер проаналізуємо результуючу таблицю та зробимо висновки.

Найкращий результат для заданого набору вхідних параметрів показав метод [72] (метод на основі трьохфакторної автентифікації та бездротових сенсорних мереж). Найгіршим в даному випадку виявився метод [47] (Метод, що використовує схожі до роумінгу засоби).

Отже, використовуючи розроблений в даній роботі аналітичний метод я зміг виокремити найкращий метод автентифікації для певних конкретних вимог.

Висновки до розділу 3

В даному розділі була створена конкретна модель загроз для пересічної мережі інтернету речей, а також створено легко розширювана та гнучка математична модель оцінювання методів автентифікації IoT.

В останньому підрозділі було зібрано інформацію про 35 різних методів автентифікації на основі аналізу статей та публікацій в авторитетних виданнях. До всіх цих даних було застосовано розроблену мною модель з довільними вхідними параметрами та обрано найркащий варіант методу автентифікації, що задовільняє заданим критеріям.

ВИСНОВКИ

Результатом виконання даної роботи є створена математично модель оцінки ефективності протоколів автентифікації в мережах інтернету речей на основі таких вхідних параметрів як наявність криптографічних

механізмів, захищеності від конкретних видів атак, важливість тих чи інших показників, суб'єктивні плюси та мінуси. Для формування конкретних результатів було розглянуто близько 60 різних методів автентифікації та виокремлено з них 35 таких, що добре показали себе в порівнянні з іншими методами в тих чи інших ситуаціях.

В розроблену мною модель легко додати інформацію про нові протоколи, а також додавати нові фактори оцінювання.

Для експеременту були змодельовані умови в яких коефіцієнту важливості криптографічних механізмів було присвоєно значення 7/10, а захищеності від конкретних атак - 3/10. Також були навмання роставлені коефіцієнти важливості захищеності від тих чи інших атак. Як результат ми отримали 5 лідерів:

1. [72] - 117
2. [68] - 81.7
3. [138] - 80.6
4. [73] - 72.7
5. [64] - 71.5

Очевидним лідером для заданих мною параметрів став метод за посиланням [72], а саме метод на основі трьохфакторної автентифікації та бездротових сенсорних мереж, що розроблений A. K. Das в 2016-ому році.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Aura T. Cryptographically generated addresses (CGA). - 2005. [Текст]

2. Bagnulo M., García-Martínez A., Azcorra A. Efficient security for IPv6 multihoming // ACM SIGCOMM Computer Communication Review. - 2005. - Т. 35. - №. 2. - С. 61-68. [Текст]

3. Bos J. W., Özen O., Hubaux J. P. Analysis and optimization of cryptographically generated addresses // Information [Текст]

4. Bagnulo M., Arkko J. Cryptographically Generated Addresses (CGA) Extension Field Format. - RFC 4581, October, 2006. [Текст]

Security. - Springer Berlin Heidelberg, 2009. - С. 17-32.

5. Arkko J., Ericsson Ed., Kempf J. Secure neighbor discovery (SEND). - RFC 3971, March, 2005. [Текст]

6. Combes J. M. et al. CGA as alternative security credentials with IKEv2: implementation and analysis // SAR-SSI'12: 7th Conference on Network Architectures and Information Systems Security. - 2012. - С. 53-59. [Текст]

7. Bagnulo M. Hash-based addresses (HBA). - 2009. [Текст]

8. Davies E., Krishnan S., Savola P. IPv6 transition / co-existence security considerations. - 2007. [Текст]

9. McGann O. IPv6 packet filtering: дис. - National University of Ireland Maynooth, 2005. [Текст]

10. Krishnan S. Handling of Overlapping IPv6 Fragments. - 2009. [Текст]

11. Deering S. E. Internet protocol, version 6 (IPv6) specification. - тисяча дев'ятсот дев'яносто вісім. [Текст]

12. Davies E., Mohacsi J. Recommendations for filtering icmpv6 messages in firewalls. - RFC 4890, May, 2007 [Текст]

13. Gont F., Ermini M., Liu W. Requirements for IPv6 Enterprise Firewalls. - April, 2014. [Текст]

14. Jankiewicz, E., Loughney, J., and T. Narten, IPv6 Node Requirements, RFC 6434, December 2011. [Текст]

15. Loughney J. IPv6 node requirements. - 2006. [Текст]

16. Korver B. The Internet IP Security PKI Profile of IKEv1 / ISAKMP, IKEv2, and PKIX. - 2007. [Текст]

17. Graveman R. et al. Using IPsec to Secure IPv6-in-IPv4 Tunnels // RFC4891, May. - 2007. [Текст]

18. Devarapalli V., Dupont F. Mobile IPv6 operation with IKEv2 and the revised IPsec architecture. - 2007. [Текст]

19. Frankel S., Krishnan S. IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap. - RFC 6071, February, 2011 року. [Текст]

20. Bi J. et al. SAVI Solution for DHCP. - May, 2014. [Текст]

21. McPherson D., Halpern J., Baker F. Source Address Validation Improvement (SAVI) Threat Scope. - 2013. [Текст]

22. Bagnulo M., Garcia-Martinez A. SEcure Neighbor Discovery (SEND) Source Address Validation Improvement (SAVI). - 2014. [Текст]

23. Mohacsi J. et al. IPv6 Router Advertisement Guard. - 2011 року. [Текст]

24. Gont F. Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard). - 2014. [Електронний ресурс]/

25. IPv6 First-Hop Security Configuration Guide, Cisco IOS Release 15S [Електронний ресурс]: Cisco Systems. - 26 Nov 2012. - Режим доступу: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/15-s/ip6f-15-s-book .pdf. [Електронний ресурс]/

26. Economou, N. (Mar, 2014). Core Security. Microsoft Windows TCP IPv6 Denial of Service Vulnerability. Retrieved from: http://blog.coresecurity.com/2014/03/25/ms14-006-microsoft-windows-tcp-ipv6-denial-of-service-vulnerability/#sthash.iBLIqqwp.dpuf [Електронний ресурс]/

27. McDowell, M. (Nev, 2009). US-CERT. Understanding Denial-of-Service Attacks. Retrieved from: http://www.us-cert.gov/ncas/tips/ST04-015 [Електронний ресурс]/

28. Q. Li and G. Cao, “Multicast authentication in the smart grid with one-time signature,” [Електронний ресурс]/ IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 686–696, 2011.

29. “I. standard 802.16m 2011,” [Електронний ресурс]/ Tech. Rep., Air

interface for broadband wireless access systems - Amendment 3: advanced air interface

30. M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. S. Shen, “A lightweight message authentication scheme for smart grid communications,” [Електронний ресурс]/ IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 675–685, 2011.

31. H.-L. Yeh, T.-H. Chen, P.-C. Liu, T.-H. Kim, and H.-W. Wei, “A secured authentication protocol for wireless sensor networks using Elliptic Curves Cryptography,” [Текст]/ Sensors, vol. 11, no. 5, pp. 4767–4779, 2011.

32. J. Cao, M. Ma, and H. Li, “A group-based authentication and key agreement for MTC in LTE networks,” [Текст]/ in Proceedings of the IEEE Global Communications Conference (GLOBECOM ’12), pp. 1017–1022, Anaheim, Calif, USA, December 2012.

33. Y.-W. Chen, J.-T. Wang, K.-H. Chi, and C.-C. Tseng, “Groupbased authentication and key agreement,” [Текст]/ Wireless Personal Communications, vol. 62, no. 4, pp. 965–979, 2012.

34. A. Fu, S. Lan, B. Huang, Z. Zhu, and Y. Zhang, “A novel groupbased handover authentication scheme with privacy preservation for mobile WiMAX networks,”[Электронный ресурс]/ IEEE Communications Letters, vol. 16, no. 11, pp. 1744–1747, 2012.

35. R. Sule, R. S. Katti, and R. G. Kavasseri, “A variable length fast message authentication code for secure communication in smart grids,”[Электронный ресурс]/ in Proceedings of the 2012 IEEE Power and Energy Society General Meeting, PES 2012, usa, July 2012.

36. A. K. Das, P. Sharma, S. Chatterjee, and J. K. Sing, “A dynamic password-based user authentication scheme for hierarchical wireless sensor networks,”[Электронный ресурс]/ Journal of Network and Computer Applications, vol. 35, no. 5, pp. 1646–1656, 2012.

37. C. Lai, H. Li, R. Lu, R. Jiang, and X. Shen, “LGTH: a lightweight group

authentication protocol for machine-type communication in LTE networks," [Электронный ресурс]/ in Proceedings of the IEEE Global Communications Conference (GLOBECOM '13), pp. 832– 837, December 2013.

38. C. Lai, H. Li, R. Lu, and X. Shen, "SE-AKA: a secure and efficient group authentication and key agreement protocol for LTE networks," [Текст]/Computer Networks, vol. 57, no. 17, pp. 3492– 3510, 2013.

39. S. Cespedes, S. Taha, and X. Shen, "A multihop-authenticated proxy mobile IP scheme for asymmetric VANETs," [Электронный ресурс]/ IEEE Transactions on Vehicular Technology, vol. 62, no. 7, pp. 3271–3286, 2013.

40. A. Wasef and X. S. Shen, "EMAP: Expedite message authentication protocol for vehicular ad hoc networks," [Электронный ресурс]/ IEEE Transactions on Mobile Computing, vol. 12, no. 1, pp. 78–89, 2013.

41. K. Xue, C. Ma, P. Hong, and R. Ding, "A temporal-credentialbased mutual authentication and key agreement scheme for wireless sensor networks," [Электронный ресурс]/ Journal of Network and Computer Applications, vol. 36, no. 1, pp. 316–323, 2013.

42. C.-T. Li, C.-Y. Weng, and C.-C. Lee, "An advanced temporal credential-based security scheme with mutual authentication and key agreement for wireless sensor networks," [Электронный ресурс]/ Sensors, vol. 13, no. 8, pp. 9589–9603, 2013.

43. Q. Jiang, J. Ma, G. Li, and L. Yang, "An enhanced authentication scheme with privacy preservation for roaming service in global mobility networks," Wireless Personal Communications, vol. 68, no. 4, pp. 1477–1491, 2013.

44. F. Wen, W. Susilo, and G. Yang, "A secure and effective anonymous user authentication scheme for roaming service in global mobility networks," Wireless Personal Communications, vol. 73, no. 3, pp. 993–1004, 2013.

45. M. Turkanovic and M. Holbl, "An improved dynamic passwordbased user authentication scheme for hierarchical wireless sensor networks,"

[Электронный ресурс]/ Elektronika ir Elektrotechnika, vol. 19, no. 6, pp. 109–116, 2013.

46. C. Lai, H. Li, R. Lu, R. Jiang, and X. Shen, “SEGR: A secure and efficient group roaming scheme for machine to machine communications between 3GPP and WiMAX networks,” [Электронный ресурс]/ in Proceedings of the 2014 1st IEEE International Conference on Communications, ICC 2014, pp. 1011–1016, aus, June 2014.

47. C. Lai, H. Li, X. Liang, R. Lu, K. Zhang, and X. Shen, “CPAL: A conditional privacy-preserving authentication with access linkability for roaming service,” [Электронный ресурс]/ IEEE Internet of Things Journal, vol. 1, no. 1, pp. 46–57, 2014.

48. A. C.-F. Chan and J. Zhou, “Cyber–Physical Device Authentication for the Smart Grid Electric Vehicle Ecosystem,” [Электронный ресурс]/ IEEE Journal on Selected Areas in Communications, vol. 32, no. 7, pp. 1509–1517, 2014.

49. H. Li, R. Lu, L. Zhou, B. Yang, and X. Shen, “An efficient Merkletree-based authentication scheme for smart grid,” [Электронный ресурс]/ IEEE Systems Journal, vol. 8, no. 2, pp. 655–663, 2014.

50. Y. Choi, D. Lee, and J. Kim, “Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography,” [Электронный ресурс]/ Sensors, vol. 14, no. 6, pp. 10081–10106, 2014.

51. M. Turkanovic, B. Brumen, and M. H ´ olbl, “A novel user ¨ authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion,” [Электронный ресурс]/ Ad Hoc Networks, vol. 20, pp. 96–112, 2014.

52. L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, and B. Qin, “Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response,” [Электронный ресурс]/ Institute of Electrical and Electronics Engineers. Transactions on Computers, vol. 65, no. 8, pp. 2562–2574, 2016.

53. X. Sun, S. Men, C. Zhao, and Z. Zhou, “A security authentication scheme in machine-to-machine home network service,”[Электронный ресурс]/ Security and Communication Networks, vol. 8, no. 16, pp. 2678–2686, 2015.

54. C. Lai, R. Lu, and D. Zheng, “SGSA: Secure group setup and anonymous authentication in platoon-based vehicular cyberphysical systems,” [Электронный ресурс]/Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Preface, vol. 9204, pp. 274–283, 2015.

55. T. W. Chim, S.-M. Yiu, V. O. Li, L. C. Hui, and J. Zhong, “PRGA: Privacy-Preserving Recording amp; Gateway-Assisted Authentication of Power Usage Information for Smart Grid,” [Электронный ресурс]/ IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 1, pp. 85–97, 2015.

56. X. Li, J. Niu, S. Kumari, J. Liao, W. Liang, and M. K. Khan, “A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity,” [Текст]/ Security and Communication Networks, vol. 9, no. 15, pp. 2643–2655, 2016.

57. D. He, N. Kumar, and N. Chilamkurti, “A secure temporalcredential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks,” [Книга]/ Information Sciences, vol. 321, Article ID 11403, pp. 263–277, 2015.

58. S. Shin, H. Yeh, and K. Kim, “An efficient secure authentication scheme with user anonymity for roaming user in ubiquitous networks,” [Электронный ресурс]/ Peer-to-Peer Networking and Applications, vol. 8, no. 4, pp. 674–683, 2015.

59. G. Prosanta and T. Hwang, “Lightweight and energy-efficient mutual authentication and key agreement scheme with user anonymity for secure communication in global mobility networks,” [Электронный ресурс]/ IEEE Systems Journal, vol. PP, no. 99, 2015.

60. M. S. Farash, S. A. Chaudhry, M. Heydari, S. M. Sajad Sadough, S.

Kumari, and M. K. Khan, “A lightweight anonymous authentication scheme for consumer roaming in ubiquitous networks with provable security,” [Электронный ресурс]/ International Journal of Communication Systems, vol. 30, no. 4, Article ID e3019, 2017.

61. C. Lai, R. Lu, D. Zheng, H. Li, and X. Sherman, “GLARM: group-based lightweight authentication scheme for resourceconstrained machine to machine communications,” [Электронный ресурс]/ Computer Networks, vol. 99, pp. 66–81, 2016.

62. D. Chen, N. Zhang, and Z. Qin, “S2M: a lightweight acoustic fingerprints based wireless device authentication protocol,” [Электронный ресурс]/ IEEE Internet of Things Journal, vol. 4, no. 1, pp. 88–100, 2017.

63. J. Shao, X. Lin, R. Lu, and C. Zuo, “A Threshold Anonymous Authentication Protocol for VANETs,” [Электронный ресурс]/ IEEE Transactions on Vehicular Technology, vol. 65, no. 3, pp. 1711–1720, 2016.

64. C. Lyu, D. Gu, Y. Zeng, and P. Mohapatra, “PBA: PredictionBased Authentication for Vehicle-to-Vehicle Communications,” [Электронный ресурс]/ IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 1, pp. 71–83, 2016.

65. L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, “Distributed Aggregate Privacy-Preserving Authentication in VANETs,” [Электронный ресурс]/ IEEE Transactions on Intelligent Transportation Systems, pp. 1–11, 2016.

66. S. Dolev, Ł. Krzywiecki, N. Panwar, and M. Segal, “Vehicle authentication via monolithically certified public key and attributes,”[Інтернет ресурс]/ Wireless Networks, vol. 22, no. 3, pp. 879–896, 2016.

67. K. Mahmood, S. Ashraf Chaudhry, H. Naqvi, T. Shon, and H. Farooq Ahmad, “A lightweight message authentication scheme for Smart Grid communications in power sector,” [Інтернет ресурс]/ Computers Electrical Engineering, vol. 52, pp. 114–124, 2016.

68. S. Kumari, X. Li, F. Wu, A. K. Das, H. Arshad, and M. K. Khan, “A user friendly mutual authentication and key agreement scheme for wireless sensor networks using chaotic maps,” [Інтернет ресурс]/ Future Generation Computer Systems, vol. 63, pp. 56–75, 2016.

69. Y. Chung, S. Choi, Y. S. Lee, N. Park, and D. Won, “An enhanced lightweight anonymous authentication scheme for a scalable localization roaming service in wireless sensor networks,” [Інтернет ресурс]/ Sensors, vol. 16, no. 10, article no. 1653, 2016.

70. R. Amin and G. Biswas, “A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks,” [Інтернет ресурс]/ Ad Hoc Networks, vol. 36, part 1, pp. 58–80, 2016.

71. P. Gope and T. Hwang, “A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks,” [Інтернет ресурс]/ IEEE Transactions on Industrial Electronics, 2016.

72. A. K. Das, “A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks,” [Інтернет ресурс]/ Peer-to-Peer Networking and Applications, vol. 9, no. 1, pp. 223–244, 2016.

73. C.-C. Chang and H.-D. Le, “A Provably Secure, Efficient, and Flexible Authentication Scheme for Ad hoc Wireless Sensor Networks,” [Інтернет ресурс]/ IEEE Transactions on Wireless Communications, vol. 15, no. 1, pp. 357–366, 2016.

74. Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen, and Y. Yang, “An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks,” [Книга]/ Journal of Network and Computer Applications, vol. 76, pp. 37–48, 2016.

75. M. S. Farash, M. Turkanovic, S. Kumari, and M. H ´ olbl, “An ¨ efficient user authentication and key agreement scheme for heterogeneous

wireless sensor network tailored for the Internet of Things environment," [Книга]/ Ad Hoc Networks, vol. 36, pp. 152–176, 2016.

76. S. Kumari, A. K. Das, M. Wazid et al., "On the design of a secure user authentication and key agreement scheme for wireless sensor networks," [Текст]/ Concurrency Computation, 2016.

77. Q. Jiang, N. Kumar, J. Ma, J. Shen, D. He, and N. Chilamkurti, "A privacy-aware two-factor authentication protocol based on elliptic curve cryptography for wireless sensor networks," [Текст]/ International Journal of Network Management, vol. 27, no. 3, Article ID e1937, 2017.

78. A. Karkouch, H. Mousannif, H. Al Moatassime, and T. Noel, "Data quality in internet of things: A state-of-the-art survey," [Текст]/ Journal of Network and Computer Applications, vol. 73, pp. 57– 81, 2016.

79. Q. Yongrui, Q. Z. Sheng, N. J. G. Falkner, S. Dustdar, H. Wang, and A. V. Vasilakos, "When things matter: a survey on datacentric internet of things," [Текст]/ Journal of Network and Computer Applications, vol. 64, pp. 137–153, 2016.

80. N. C. Luong, D. T. Hoang, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Data Collection and Wireless Communication in Internet of Things (IoT) Using Economic Analysis and Pricing Models: A Survey," [Электронный ресурс]/ IEEE Communications Surveys & Tutorials, vol. 18, no. 4, pp. 2546–2590, 2016.

81 S. Bandyopadhyay, M. Sengupta, S. Maiti, and S. Dutta, "A survey of middleware for internet of things," [Электронный ресурс]/ in Recent Trends in Wireless and Mobile Networks, vol. 162 of Communications in Computer and Information Science, pp. 288–296, Springer, Berlin, Germany, 2011.

82. M. A. Chaqfeh and N. Mohamed, "Challenges in middleware solutions for the internet of things," [Электронный ресурс]/ in Proceedings of the 13th International Conference on Collaboration Technologies and Systems (CTS '12), pp. 21–26, Denver, Colo, USA, May 2012.

83. T. Teixeira, S. Hachem, V. Issarny, and N. Georgantas, "Service

oriented middleware for the internet of things: A perspective (invited paper),” [Наукова робота]/ Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Preface, vol. 6994, pp. 220–229, 2011.

84. M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, “Middleware for Internet of things: a survey,” [Электронный ресурс]/ IEEE Internet of Things Journal, vol. 3, no. 1, pp. 70–95, 2016.

85. A. Zanella, N. Bui, A. P. Castellani, L. Vangelista, and M. Zorzi, “Internet of things for smart cities,” [Электронный ресурс]/ IEEE Internet of Things Journal, vol. 1, no. 1, pp. 22–32, 2014.

86. E. Ahmed, I. Yaqoob, A. Gani, M. Imran, and M. Guizani, “Internet-of-things-based smart environments: State of the art, taxonomy, and open research challenges,” [Электронный ресурс]/ IEEE Wireless Communications Magazine, vol. 23, no. 5, pp. 10–16, 2016.

87. A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, and T. Razafindralambo, “A survey on facilities for experimental internet of things research,” [Электронный ресурс]/ IEEE Communications Magazine, vol. 49, no. 11, pp. 58–67, 2011.

88. L. Mainetti, L. Patrono, and A. Vilei, “Evolution of wireless sensor networks towards the Internet of Things: a survey,” [Электронный ресурс]/ in Proceedings of the 19th International Conference on Software, Telecommunications and Computer Networks (SoftCOM ’11), pp. 16–21, September 2011.

89. R. Roman, C. Alcaraz, J. Lopez, and N. Sklavos, “Key management systems for sensor networks in the context of the Internet of Things,” [Электронный ресурс]/ Computers Electrical Engineering, vol. 37, no. 2, pp. 147–159, 2011.

90. C. C. Aggarwal, N. Ashish, and A. Sheth, “The Internet of Things: A Survey from the Data-Centric Perspective,” [Электронный ресурс]/ in

Managing and Mining Sensor Data, pp. 383–428, Springer US, Boston, MA, 2013.

91. N. Bizanis and F. A. Kuipers, “SDN and virtualization solutions for the internet of things: a survey,” [Электронный ресурс]/ IEEE Access, vol. 4, pp. 5591– 5606, 2016.

92. P. Rawat, K. D. Singh, and J. M. Bonnin, “Cognitive radio for M2M and Internet of Things: A survey,” [Электронный ресурс]/ Computer Communications, vol. 94, pp. 1–29, 2016.

93. D. Bandyopadhyay and J. Sen, “Internet of things: applications and challenges in technology and standardization,” [Электронный ресурс]/ Wireless Personal Communications, vol. 58, no. 1, pp. 49–69, 2011.

94. D. Miorandi, S. Sicari, F. de Pellegrini, and I. Chlamtac, “Internet of things: vision, applications and research challenges,” [Электронный ресурс]/ Ad Hoc Networks, vol. 10, no. 7, pp. 1497–1516, 2012.

95. Z. G. Sheng, S. S. Yang, Y. F. Yu, A. V. Vasilakos, J. A. McCann, and K. K. Leung, “A survey on the ietf protocol suite for the internet of things: standards, challenges, and opportunities,” [Электронный ресурс]/ IEEE Wireless Communications Magazine, vol. 20, no. 6, pp. 91– 98, 2013.

96. I. Ishaq, D. Carels, G. Teklemariam et al., “IETF standardization in the field of the internet of things (IoT): a survey,” [Электронный ресурс]/ Journal of Sensor and Actuator Networks, vol. 2, no. 2, pp. 235–287, 2013.

97. M. R. Palattella, N. Accettura, X. Vilajosana et al., “Standardized protocol stack for the internet of (important) things,” [Электронный ресурс]/ IEEE Communications Surveys & Tutorials, vol. 15, no. 3, pp. 1389– 1406, 2013.

98. C.-W. Tsai, C.-F. Lai, and A. V. Vasilakos, “Future internet of things: open issues and challenges,” [Электронный ресурс]/ Wireless Networks, vol. 20, no. 8, pp. 2201–2217, 2014.

99. M. C. Domingo, “An overview of the internet of things for people with disabilities,” [Электронный ресурс]/ Journal of Network and Computer

Applications, vol. 35, no. 2, pp. 584–596, 2012.

100. L. D. Xu, W. He, and S. Li, “Internet of things in industries: A survey,” [Электронный ресурс]/ IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2233–2243, 2014.

101. C. Perera, C. H. Liu, S. Jayawardena, and M. Chen, “A survey on internet of things from industrial market perspective,” [Электронный ресурс]/ IEEE Access, vol. 2, pp. 1660–1679, 2014.

102. Z. Bi, L. D. Xu, and C. Wang, “Internet of things for enterprise systems of modern manufacturing,” [Электронный ресурс]/ IEEE Transactions on Industrial Informatics, vol. 10, no. 2, pp. 1537–1546, 2014.

103. M. R. Abdmeziem, D. Tandjaoui, and I. Romdhani, “Architecting the internet of things: state of the art,” [Электронный ресурс]/ pp. 55–75, 2016.

104. D. Zhang, L. T. Yang, and H. Huang, “Searching in Internet of Things: Vision and challenges,” [Электронный ресурс]/ in Proceedings of the 9th IEEE International Symposium on Parallel and Distributed Processing with Applications, ISPA 2011, pp. 201–206, kor, May 2011.

105. H. Suo, J. Wan, C. Zou, and J. Liu, “Security in the internet of things: a review,” [Электронный ресурс]/ in Proceedings of the International Conference on Computer Science and Electronics Engineering (ICCSEE ’12), pp. 648–651, Hangzhou, China, March 2012.

106. R. Roman, J. Zhou, and J. Lopez, “On the features and challenges of security and privacy in distributed internet of things,” [Книга]/ Computer Networks, vol. 57, no. 10, pp. 2266–2279, 2013.

107. Z. Yan, P. Zhang, and A. V. Vasilakos, “A survey on trust management for Internet of Things,” [Электронный ресурс]/ Journal of Network and Computer Applications, vol. 42, pp. 120–134, 2014.

108. Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, “Security of the internet of things: perspectives and challenges,”[Электронный ресурс]/ Wireless Networks, vol. 20, no. 8, pp. 2481–2501, 2014.

109. S. Chabridon, R. Laborde, T. Desprats, A. Oglaza, P. Marie, and S. M. Marquez, “A survey on addressing privacy together with quality of context for context management in the Internet of Things,” [Электронный ресурс]/ Annals of Telecommunications-Annales des Telecommunications ´ , vol. 69, no. 1-2, pp. 47–62, 2014.

110. J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, “Privacy in the internet of things: threats and challenges,” [Книга]/Security and Communication Networks, vol. 7, no. 12, pp. 2728–2742, 2014.

111. W. Xie, Y. Tang, S. Chen, Y. Zhang, and Y. Gao, “Security of Web of Things: A Survey (Short Paper),” [Электронный ресурс]/ in Advances in Information and Computer Security, vol. 9836 of Lecture Notes in Computer Science, pp. 61–70, Springer International Publishing, Cham, 2016.

112. S. L. Keoh, S. S. Kumar, and H. Tschofenig, “Securing the internet of things: a standardization perspective,” [Электронный ресурс]/ IEEE Internet of Things Journal, vol. 1, no. 3, pp. 265–275, 2014.

113. S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, privacy and trust in Internet of Things: the road ahead,” [Книга]/ Computer Networks, vol. 76, pp. 146–164, 2015.

114. J. Granjal, E. Monteiro, and J. Sa Silva, “Security for the internet of things: a survey of existing protocols and open research issues,” [Электронный ресурс]/ IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1294–1312, 2015.

115. A.-R. Sadeghi, C. Wachsmann, and M. Waidner, “Security and privacy challenges in industrial internet of things,” [Электронный ресурс]/ in Proceedings of the 52nd ACM/EDAC/IEEE Design Automation Conference (DAC ’15), pp. 1–6, IEEE, San Francisco, Calif, USA, June 2015.

116. K. T. Nguyen, M. Laurent, and N. Oualha, “Survey on secure communication protocols for the Internet of Things,” [Электронный ресурс]/ Ad Hoc Networks, vol. 32, article no. 1181, pp. 17–31, 2015.

117. J. Singh, T. Pasquier, J. Bacon, H. Ko, and D. Eyers, “Twenty Security Considerations for Cloud-Supported Internet of Things,” [Электронный ресурс]/ IEEE Internet of Things Journal, vol. 3, no. 3, pp. 269– 284, 2016.

118. S. Li, T. Tryfonas, and H. Li, “The Internet of Things: a security point of view,” [Электронный ресурс]/ Internet Research, vol. 26, no. 2, pp. 337–359, 2016.

119. D. Airehrour, J. Gutierrez, and S. K. Ray, “Secure routing for internet of things: A survey,” [Электронный ресурс]/ Journal of Network and Computer Applications, vol. 66, pp. 198–213, 2016.

120. X. Jia, Q. Feng, T. Fan, and Q. Lei, “RFID technology and its applications in Internet of Things (IoT),” [Электронный ресурс]/ in Proceedings of the 2012 2nd International Conference on Consumer Electronics, Communications and Networks, CECNet 2012, pp. 1282–1285, chn, April 2012.

121. D. He and S. Zeadally, “An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography,” [Электронный ресурс]/ IEEE Internet of Things Journal, vol. 2, no. 1, pp. 72–83, 2015.

122. L. Atzori, A. Iera, G. Morabito, and M. Nitti, “The social internet of things (SIoT)—when social networks meet the internet of things: concept, architecture and network characterization,” [Книги]/ Computer Networks, vol. 56, no. 16, pp. 3594–3608, 2012.

123. B. Guo, D. Zhang, Z. Wang, Z. Yu, and X. Zhou, “Opportunistic IoT: exploring the harmonious interaction between human and the internet of things,” Journal of Network and Computer Applications, vol. 36, no. 6, pp. 1531–1539, 2013.

124. A. M. Ortiz, D. Hussein, S. Park, S. N. Han, and N. Crespi, “The cluster between internet of things and social networks: Review and research challenges,” [Электронный ресурс]/ IEEE Internet of Things Journal, vol. 1, no. 3, pp. 206–215, 2014.

125. L. Maglaras, A. Al-Bayatti, Y. He, I. Wagner, and H. Janicke, “Social Internet of Vehicles for Smart Cities,” [Электронный ресурс]/ Journal of Sensor and Actuator Networks, vol. 5, no. 1, p. 3, 2016.

126. H.-D. Ma, “Internet of things: objectives and scientific challenges,” [Электронный ресурс]/ Journal of Computer Science and Technology, vol. 26, no. 6, pp. 919–924, 2011.

127. F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, “Fog computing and its role in the internet of things,” [Электронный ресурс]/ in Proceedings of the 1st ACM Mobile Cloud Computing Workshop, MCC 2012, pp. 13–15, fin, August 2012.

128. A. Botta, W. De Donato, V. Persico, and A. Pescape, “On the integration of cloud computing and internet of things,” [Электронный ресурс]/ in Proceedings of the 2nd International Conference on Future Internet of Things and Cloud (FiCloud ’14), pp. 23–30, Barcelona, Spain, August 2014.

129. A. Whitmore, A. Agarwal, and L. Da Xu, “The internet of things—a survey of topics and trends,” [Электронный ресурс]/ Information Systems Frontiers, vol. 17, no. 2, pp. 261–274, 2015.

130. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of things: a survey on enabling technologies, protocols, and applications,” [Электронный ресурс]/ IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.

131. A. Botta, W. de Donato, V. Persico, and A. Pescape, “Integration ´ of cloud computing and internet of things: a survey,” [Электронный ресурс]/ Future Generation Computer Systems, vol. 56, pp. 684–700, 2016.

132. J. Liu, H. Shen, and X. Zhang, “A survey of mobile crowdsensing techniques: A critical component for the internet of things,”[Электронный ресурс]/ in Proceedings of the 25th International Conference on Computer Communications and Networks, ICCCN 2016, usa, August 2016.

133. D. Gil, A. Ferrandez, H. Mora-Mora, and J. Peral, “Internet of ´ things:

a review of surveys based on context aware intelligent services," [Электронный ресурс]/ Sensors, vol. 16, no. 7, article 1069, 2016.

134. M. D´ıaz, C. Mart´ın, and B. Rubio, "State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing," [Электронный ресурс]/ Journal of Network and Computer Applications, vol. 67, pp. 99–117, 2016.

135. C. Tsai, C. Lai, M. Chiang, and L. T. Yang, "Data mining for internet of things: a survey," [Электронный ресурс]/ IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 77–97, 2014.

136. F. Chen, P. Deng, J. Wan, D. Zhang, A. V. Vasilakos, and X. Rong, "Data mining for the internet of things: Literature review and challenges," [Электронный ресурс]/ International Journal of Distributed Sensor Networks, vol. 2015, Article ID 431047, 2015.

137. H. Zhu, X. Lin, Y. Zhang, and R. Lu, "Duth: A user-friendly dual-factor authentication for Android smartphone devices,"[Книга]/ Security and Communication Networks, vol. 8, no. 7, pp. 1213– 1222, 2015.

138. D. Li, Z. Aung, J. R. Williams, and A. Sanchez, "Efficient authentication scheme for data aggregation in smart grid with fault tolerance and fault diagnosis," [Электронный ресурс]/ in Proceedings of the IEEE PES Innovative Smart Grid Technologies (ISGT '12), pp. 1–8, IEEE, January 2012.

139. H. Nicanfar, P. Jokar, and V. C. M. Leung, "Smart grid authentication and key management for unicast and multicast communications,"[Электронный ресурс]/ in Proceedings of the IEEE Power and Energy Society'sInnovative Smart Grid Technologies Asia 2011 Conference,ISGT Asia 2011, aus, November 2011.

140. T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "PASS: Privacy-preserving authentication scheme for smart grid network,"[Электронный ресурс]/ in Proceedings of the 2011 IEEE 2nd International Conference on Smart Grid Communications, SmartGridComm 2011, pp. 196–201, bel, October 2011.

141. M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. Shen, “Towards a light-weight message authentication mechanism tailored for Smart Grid communications,”[Электронный ресурс]/ in Proceedings of the 2011 IEEE Conference on Computer CommunicationsWorkshops, INFOCOM WKSHPS 2011, pp. 1018–1023, chn, April 2011.

142. H. Nicanfar, P. Jokar, K. Beznosov, and V. C. M. Leung, “Efficient authentication and key management mechanisms for smart grid communications,” [Электронный ресурс]/ IEEE Systems Journal, vol. 8, no. 2, pp. 629– 640, 2014.