ТЕХНИЧЕСКИ УНИВЕРСИТЕТ – СОФИЯ

Факултет по Телекомуникации

Катедра Комуникационни мрежи

Маг. инж. Джадхав Сантош Пандуранг

ПОДОБРЯВАНЕ НА СИГУРНОСТТА И ЕФЕКТИВНОСТТА НА IoT УСТРОЙСТВА С ОГРАНИЧЕНИ РЕСУРСИ

А В Т О Р Е Ф Е Р А Т

на дисертация за придобиване на образователна и научна степен

"ДОКТОР"

Област: 5. Технически науки

Професионално направление: 5.3 Комуникационна и компютърна техника

Научна специалност: Комуникационни мрежи и системи

Научни ръководители: доц. д-р инж. Георги Райчев Балабанов
проф. дн инж. Владимир Костадинов Пулов

СОФИЯ, 2021 г.

Дисертационният труд е обсъден и насочен за защита от Катедрения съвет на катедра „Комуникационни мрежи“ към Факултет по Телекомуникации на ТУ–София на редовно заседание, проведено на 31.05.2021 г. (Протокол № 11).

Публичната защита на дисертационния труд ще се състои на 18.10.2021 г. от 13,00 часа в Конферентната зала на БИЦ на Технически университет – София на открито заседание на научното жури, определено със заповед № ОЖ-5.3-26 от 29.06.2021 г. на Ректора на ТУ-София в състав:

1. Проф. д-р Георги Илиев – председател
2. Доц. д-р инж. Георги Балабанов – научен секретар
3. Проф. д-р инж. Иван Куртев
4. Доц. д-р инж. Валентина Маркова
5. Доц. д-р инж. Габриела Атанасова

Рецензенти:

1. Проф. д-р Георги Илиев
2. Доц. д-р инж. Габриела Атанасова

Материалите по защитата са на разположение на интересуващите се в канцеларията на Факултет по Телекомуникации на ТУ–София, блок №1, кабинет № 1254.

Дисертантът е редовен докторант към катедра „Комуникационни мрежи“ на факултет по Телекомуникации. Изследванията по дисертационната разработка са направени от автора.

Автор: маг. инж. Джадхав Сантош Пандуранг
Заглавие: Подобряване на сигурността и ефективността на IoT устройства с ограничени ресурси
Тираж: 30 броя
Отпечатано в ИПК на Технически университет – София

I. ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

Актуалност на проблема

Бързото нарастване на IoT бизнеса доведе до прилагане на все повече криптографски методи за защита. Предприемат се различни подходи, за да се гарантира информацията, генерирана от IoT устройства, и по-обширната сигурност на структурата на IoT мрежи, част от която е новата дейност "лека криптография". Това изисква формирането на нови изчисления и методи, които могат да се справят с основните схеми с ниска мощност. Тестът показва, че много IoT устройства използват неподходяща електрическа мощност и хардуер, който безспорно е по-ограничен дори чиповете на повечето съвременни телефони, а методите за криптиране обикновено изискват по-голяма мощност от това. В този смисъл, целта трябва да бъде насочена към подходи с „лека криптография“. Жизнеспособните норми трябва да донесат много характерно устройство, приложимо за широк кръг потребители.

Различните области на приложението на IoT генерират много ценни данни, които могат да бъдат свързани със здравето на потребителите или данни за парични транзакции, които са полезни за различни приложения и решения. Данните могат да бъдат поверителни и чувствителни и трябва да се полага грижи за тях. Поради бързия си растеж в IoT, той стана по-податлив на различни кибер атаки. Следователно от голямо значение е да се проучат мерките за сигурност, като се внимава това да не влияе на ефективността на устройствата на IoT. Поради огромния асортимент и хетерогенност на IoT устройствата и целите за сигурност на приложенията, които ги използват, леките криптографски алгоритми за IoT демонстрират предизвикателни задачи, които трябва да бъдат решени. Съществуват предизвикателства както по отношение на осигуряването на задоволителна сигурност, така и според ефекта върху изпълнението на устройството, изискващи критични компромиси спрямо нивата на мрежова сигурност, които използваме. Такива компромиси могат да ограничат вида на използваните IoT устройства, който можем да приложим в дългосрочен план, във всеки случай, докато не бъде създадено защитено олекотено устройство.

Web of Things (WoT) се превърна в друга идея за текущия напредък в кореспонденцията и нов мироглед. Идеята е да се свържат неща (например RFID етикети, сензори, устройства и т.н.), които могат да си сътрудничат и да обменят информация помежду си навсякъде в мрежата. С развитието на IoT, обемът на информацията, обменяна между асоцииращите IoT устройства, се разширява с голям обхват поради нарастващия брой на свързаните обекти. По-голямата част от IoT устройствата са устройства, които се грижат за секретна и чувствителна информация. Следователно използването на обикновени криптографски техники е неприемливо поради многобройни проблеми и трудности като ограничена изчислителна сила, памет, енергийни активи, разходи за изпълнение и предпоставка за сигурност. За това са представени леки криптографски методи. Извършвата се можество изследвания, за да намерят разумно решение, което отговаря на специфичните нужди на приложението IoT

Бързото развитие на приложения на IoT разширява обхвата на предаваната информация, довеждайки до все по-голямо искане на администрациите за сигурност като тайна на информацията, честност и проверка на източника. Във всеки случай, усилията за използване на механизми за сигурност, които се изпълняват в

конвенционалните мрежи, вероятно ще предизвикат нежелано въздействие поради пречките, свързани с оборудването. Най-важните режийни разходи се идентифицират с използването на енергия или потенциално нарастване на закъсненията за кореспонденция. Друго притеснение е обикновено по-голямото използване на паметта, което може да бъде нарушено от достъпната памет на приложението и степента и на използване. По този начин, една от основните трудности при предаването на инструментите за сигурност през IoT е да се ограничи противоречието между използването на активите и идеалната сигурност.

След преглед на състоянието на техниката, свързано със сигурността на устройствата на IoT, може да се заключи, че като цяло много устройства с IoT имат ограничени възможности за съхранение, памет и обработка и често трябва да могат да работят с по-ниска мощност, например, защото работят на батерии. Подходите за сигурност, които разчитат силно на криптирането, не са подходящи за такива ограничени устройства, тъй като те не са способни да извършват достатъчно бързо сложно криптиране и декриптиране, за да могат да предават данни сигурно в реално време. И така, има нужда от изключително сигурни и леки алгоритми за криптография, които ще разгледат проблема с IoT устройствата, т.е.разглеждане на проблема с ниска мощност, по-ниска изчислителна сложност, ефективност и скорост. За да се осигури сигурност на устройството за поверителност на данните, която е в основата на сигурността на IoT услугата, трябва да се обмисли разработването на лека технология за криптиране, подходяща за устройства с ограничени ресурси.

Изследват се различни съвети и техники, за да се решат проблемите със сигурността в IoT, а проектирането на леки алгоритми за криптография са едно от усилията. Но има необходимост от разработване и проучване на изключително сигурен и лек механизъм, който е по-подходящ за леките устройства с ресурси в IoT и може да се справи с различните атаки срещу леки алгоритми за криптиране. Забелязва се, че проблемите със сигурността могат да бъдат решени по-ефективно, като се използват по-нови леки алгоритми за криптиране за устройства с ограничени ресурси.

В дисертационният труд са разгледани проектирането и внедряването на различни техники и алгоритми, които са се оказали ефективни за повишаване на сигурността и ефективността на устройствата с ограничени ресурси. Криптографията за хиперелиптична крива на асиметричен алгоритъм (HECC), заедно с протокол за нулево знание (ZKP) за удостоверяване, заедно с техниката на криптиране, се използват за намаляване на изчислителните разходи на криптографския процес. Тази работа се фокусира основно върху повишаване на сигурността и ефективността на малките леки устройства в IoT, които също се наричат устройства с ограничени ресурси, тъй като имат ниска изчислителна мощност.

За да се подобри сигурността в IoT, има нужда от изследвания за разработване на изключително сигурен и ефективен лек алгоритъм за криптиране. Като се разгледа литературното проучване на различни леки криптографски алгоритми и различни атаки, пред които е изправена IoT системата, има нужда от подобрение в механизма за сигурност. Традиционните техники имат няколко недостатъка от по-висок размер на ключа, по-големи разходи за изчисление и т.н., което е основен проблем за устройствата с ограничени ресурси в IoT среда.

Цел на дисертационния труд, основни задачи и методи за изследване

Целта на научните изследвания в дисертационния труд е да се проектира и разработи ефективен алгоритъм за откриване на нетипични стойности при поточно предаване на данни в реално време при ограничения на използваната памет с висока точност и минимално време за изпълнение.

За постигане на поставената цел са дефинирани следните задачи:

1. Да се проучат различните техники за откриване на нетипични стойности и да се оцени тяхната ефективност.

2. Да се проектира и разработи метод за откриване на нетипични стойности, който може да оперира с поточни данни, може да се изпълнява при ограничения в използваната памет и при невъзможност всички генерирани в реално време стойности да се съхраняват, има висока точност на определяне на отклонения и аномалии в данните, изчислително ефективен е и осигурява минимално време за изпълнение.

3. Да се оцени производителността на проектирания и раработен метод по отношение изпозлвана памет, време за изпълнение и точност на определяне на отклонения и аномалии в поточните данни.

Методологична основа

Темата на дисертационния труд е в областта на приложението на криптиращите алгоритми в IoT. За решаването на поставените задачи са приложени различни техники осигуряващи ефективност с по-малко изчислителни разходи заедно с повишено или същото ниво на сигурност. Приложени са техники за криптиране на знаци и използването на леки криптографски алгоритми, като методи за увеличаване на ефективността на устройствата с ограничени ресурси.

Научна новост

Интернет на нещата (IoT) е определен като критичен фактор в изчислителните системи, който влияе върху производителността, независимо от приложението му. Основният фокус на изследването е върху защитата на данните. IoT системите продължават да проникват по-дълбоко в личния ни живот. Системите чуват, обработват и запазват всички форми на данни в нашето ежедневие. Този сценарий представя редица проблеми със защитата и поверителността. Дизайнерите на системите избират добре установени механизми за защита на данните, които гарантират поверителност и цялост на данните, особено за приложения, работещи за системи с ограничени ресурси. Те обръщат особено внимание на успеха на редица алгоритми за хеширане, криптографски блокове и поточни шифри, кодове за удостоверяване на съобщения, процеси на подписване и управление на ключове. Получените резултати насърчават изчисляването на праговете за производителност / защита на данните и улесняват проектирането и изпълнението на праговете за производителност / защита на данните, като предоставят стойности на ограничения и пропускателна способност за създаване на стабилна рамка на IoT.

Всяка ситуация на приложение на IoT изисква конкретни гаранции за производителност от IoT инфраструктурата, внедрена в този сценарий (като латентност, загуба, консумация на енергия и т.н.). Например стойностите на нивата на вибрации в частите на самолета в полет трябва да бъдат сведени до минимум. За наблюдение в реално време данните трябва да се предават на сървър с възможно най-малко латентност. За да се осигури наличност на процесора за други, може би по-важни операции на IoT възел, консумацията на процесор на конкретен процес не

трябва да надвишава зададена стойност. Миниомален спад в тези параметри на ефективността може да доведе до нарушения на споразумението за ниво на услугата (SLA) и сериозни финансови санкции, загуби в приходите и функционалността. Първата стъпка е да се потвърди, че внедрената IoT архитектура отговаря на обещанията на показателите за производителност и че техните стойности са в рамките на предвидения диапазон. Следващата стъпка е да се изчислят тези показатели. Тези параметри на производителността трябва да се измерват от IoT системата и мениджърите на мрежата, за да поемат реактивни задължения за отстраняване на неизправности, като откриване и локализиране на виновни нарушителни потоци за създаване на закъснения и спадане на производителността, и определяне кои процеси доминират в процесора на IoT възел. Те също изискват тези показатели, за да открият активно всеки потенциален отказ. Измерванията на производителността на IoT обхващат както измерванията за качество на услугата (QoS) на мрежата на IoT като латентност, загуба и пропускателна способност, така и мерките за използване на ресурсите на IoT възел (RU) като потреблението на енергия, достъп и използване на диска.

Изчисляването на тези показатели за производителност не трябва да се извършва в крйното устройство, тъй като тези устройства обикновенно разполагат с по-ниски ресурси за справяне с тази задача. Така че, тази задача за измерване на показателите за производителност трябва да се извършва в облака или на хоста. Второ, той трябва да може да прави финни измервания, а не просто агрегирани измервания на изискваната статистика за ефективността, използване на процесора от всички процеси на IoT възел, закъснение на всички пакети, напускащи IoT възел. Той трябва да може да се свързва с облачна платформа, но също така трябва да може да получава мерки за данни, взети на базата на показатели за всеки отделен случай. като използването на процесора на всеки процес на IoT възел и средното закъснение на всеки поток между IoT възела и облачната платформа за облак и т.н. Терминът екземпляр ще се използва за означаване на един обект, който има необходимата метрика на производителността, поток на мрежата или активност на процесора, като за тези обстоятелства желаните показатели за ефективност могат да бъдат съответно размер на потока и време до завършване. Използване на процесора, от друга страна. Измерванията с по-фино зърно се наричат финозърнести измервания, тези измервания са важни, защото, дори ако общата стойност на метриката на ефективността изглежда нормална, стойността й за конкретен случай може да не е напълно извън обичайното измерване, например Microburst (едновременни кратки серии от данни от значителна подгрупа от IoT възли) могат да доведат до загуби на пакети за някои потоци на IoT шлюзове, дори ако средната пропускателна способност на шлюза е в границите на възможностите на шлюза. Въпреки че оценката на показателите за производителност в IoT е нова и сравнително неизползвана тема, много работа е извършена по оценка на показателите за производителност в традиционните мрежи и центрове за данни, като се подчертава необходимостта от оценка на показателите за производителност на мрежата в нарастващите IoT мрежи. Въпреки че са представени многобройни подходи за измерване на показатели за изпълнение в традиционните мрежи и системи, те са неподходящи за дизайна на IoT по две причини. Като начало, по-голямата част от съществуващите системи не са пасивни, т.е. те изпълняват активни действия за събиране на измервания, като например използват активни сонди. Въпреки че активните схеми работят добре с традиционните мрежови устройства, те са

проблематични за IoT възлите, тъй като пречат на редовните операции на възлите, а ограничените ресурси на такива възли затрудняват извършването на такива спомагателни активни действия, като същевременно гарантират, че нормалните им операции ще останат незасегнати. Второ, настоящите подходи за пасивно измерване за традиционните мрежи и системи консумират много изчислителни ресурси и памет. Moshref et al. например, използва количеството изчислителни ресурси в сървърите на центрове за данни, за да създаде рамка за измерване и откриване на прояви на интерес. Обикновено изчислителните ресурси не са проблем на традиционните сървъри, но те са оскъдни за IoT възлите. В резултат на това IoT възлите не могат да използват традиционни методи за измерване, без да пречат на нормалните им дейности. В резултат на това се изисква рамка, която е създадена с мисъл за IoT архитектури.

Практическа приложимост

Предложените подходи за откриване на локални отклонения в поточни данни могат да бъдат изпозлвани за определяне на аномалии и отклонения в системи, при който данните се генерират динамично, изчисленията се извършват в реално време при ограничение на изчислителните ресурси и капацитета на използваната памет и се изисква висока точност при определянето на нетипични стойности.

Структура и обхват на дисертационния труд

Дисертационният труд е с обем от 94 страници, включително Въведение, Четири от главите за решаване на формулираните основни задачи, списък на основните приноси, списък с научни трудове по темата на дисертацията и списък с референции. Цитираният в дипломната работа списък на литературата включва 93 литературни източници. Работата включва общо шестнадесет фигури и седем таблици. Номерата на фигурата и таблиците в автореферата съответстват на тези в дисертационният труд.

Публикуване на резултатите от дисертационното изследване

Основните постижения и резултати от работата са публикувани в 4 научни статии, от които една е самостоятелна. Изследователските статии са публикувани в Journal of Mobile Multimedia, IEEE конференция, списание за ИТ в индустрията и 5-та Международна конференция за напредъка в изчислителната техника и науките за данни (ICACDS) 2021, спонсорирана от Springer.

II. СЪДЪРЖАНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

ГЛАВА 1. Литературен обзор

След преглед на състоянието на техниката, свързано със сигурността на IoT устройствата, може да се заключи, че като цяло много IoT устройства имат ограничени възможности за съхранение, памет и обработка и често трябва да могат да работят с по-ниска мощност, например, защото работят на батерии. Подходите за сигурност, които разчитат на криптирането, не са подходящи за такива ограничени устройства, тъй като те не са способни да извършват достатъчно бързо сложното криптиране и декриптиране, за да могат да предават данни сигурно в реално време. И така, има нужда от изключително сигурни и леки алгоритми за криптография, които да решат проблема с IoT устройствата, т.е.разглеждане на проблема с ниска мощност, по-ниска изчислителна сложност, ефективност и скорост. За да се осигури сигурност на устройството за поверителност на данните, която е в основата на сигурността на IoT услугата, трябва да се обмисли разработването на лека технология за криптиране, подходяща за устройства с ограничени ресурси.

Изследват се различни съвети и техники, за да се решат проблемите със сигурността в IoT, а проектирането на леки алгоритми за криптография са едно от усилията. Но има необходимост от разработване и проучване на изключително сигурен и лек механизъм, който е по-подходящ за леките устройства и може да се справи с различните атаки. Забелязва се, че проблемите със сигурността могат да бъдат решени по-ефективно, като се използват по-нови леки алгоритми за криптиране за устройства с ограничени ресурси.

За да се подобри сигурността в IoT, има нужда от изследвания за разработване на много сигурен и ефективен лек алгоритъм за криптиране. Като се разгледа литературното проучване на различни леки криптографски алгоритми и различни атаки, пред които е изправена IoT системата, има нужда от подобрение в механизма за сигурност. Традиционните техники имат няколко недостатъка - по-висок размер на ключа, по-големи разходи за изчисления и т.н., което е основен проблем за устройствата с ограничени ресурси в IoT среда.

Глава 1 има следните два приноса:

- Представено е подробно проучване и анализ на леки криптографски алгоритми и техните проблеми със сигурността, като се вземат предвид изискванията за сигурност на различни нива. В проучването проблемите със сигурността на леките алгоритми и наличните решения се разглеждат от началните им етапи на развитие.
- В резултат на анализа на състоянието на техниката се идентифицират основните изисквания за сигурност, свързани с ефективността и сигурността на криптографията на леки критерии и въз основа на това изследване се формулират целта и задачите на дипломната работа.

Целите на изследването, които са в съответствие с целта на дипломната работа, са изброени по-долу.

- Да проучат различните изисквания за сигурност на ресурсите с ограничени ресурси, заедно с наличните решения за сигурност и да намери критичните области в IoT, където е необходимо подобряване на сигурността.
- Да се подобри цялостната сигурност на IoT, като се предложи усъвършенстван криптографски алгоритъм, който отнема по-малко изчислителна мощност и осигурява по-високо ниво на сигурност.
- Да се разработи бърз, сигурен и ефективен механизъм за проверка на потребителя, който прилага протокол с нулево знание за целите на проверката.

ГЛАВА 2. Подобряване на сигурността и ефективността на устройствата с ограничени ресурси в IoT, използващи криптография на хипер елиптична крива

В глава 2 са представени различните проблеми свързани със сигурността при работа с устройства с ограничени ресурси в IoT. Винаги се препоръчва да се използват леки протоколи за всички видове криптография, използвани за защита на устройствата от заплахи. Това определено ще направи системата по-ефективна и сигурна. Някои специфични видове елиптични криви са известни като хиперелиптични криви. В сравнение с други криптографски алгоритми, използващи криптография, базирана на елиптична крива, значително ще намали размера на ключа на криптирането. Следователно прилагането на този тип криптография в системи, които се нуждаят от висока сигурност и по-малък размер на ключа, е намерило голямо внимание. Хиперелиптичните криви помагат за намаляване на дължината на ключа. Правят се много изследвания по отношение на подобряването на изчисленията, хардуерната и софтуерната реализация на тези криви, тяхната сигурност и устойчивост срещу атаки. Тази глава изследва и анализира изследвания, направени за сигурността и ефективността на хиперелиптичните криви. HECC може да се използва за разработване на криптосистема, която може да подписва и удостоверява документи и да криптира / дешифрира съобщения ефективно за ограничени устройства в безжични мрежи. Сигурността на криптографията на елиптичната крива зависи от трудността при намиране на стойността на k, дадена Kp. Където k е голямо число, а P е произволна точка от елиптичната крива. Това е така наречената дискретна логаритмична задача на Елиптичната крива (ECDLP). Параметрите на елиптичната крива за криптографските схеми трябва да бъдат внимателно подбрани, за да се противопоставят на всички известни атаки на ECDLP. През по-голямата част от времето, откакто бяха предложени, беше широко разпространено мнението, че HECC носи значително наказание за производителност в сравнение с криптосистемите с елиптична крива (ECC) и следователно не са твърде привлекателни за практически приложения. Съвсем наскоро бяха направени подобрения, главно ограничени до криви от род 2

Изследвани са няколко леки алгоритми, които могат да се използват за намаляване на изчисленията и консумацията на батерията, което ще помогне на IoT устройствата да повишат ефективността и сигурността. Представени са различните проблеми със сигурността при работа с устройства с ограничени ресурси в IoT.

Тази глава има следните приноси, свързани с повишаването на сигурността и ефективността на устройства с ограничени ресурси в IoT.

• IoT устройствата са с лек характер и имат по-ниска изчислителна мощност и поради това се нуждаят от по-малко режийни разходи, за да ги направят ефективни. HECC установява, че е по-подходящ в такъв сценарий и може да бъде предложен за сигурен трансфер на данни в IoT системи.

• Анализът на различните налични хиперелиптични криви се извършва, за да се установи коя крива е подходяща за ограниченото от ресурси приложение. Резултатите от анализа са представени в таблица 2.1.

Security level	Elliptic curve	HECC Genus 2	HECC Genus 3
256	94	47	32
512	128	64	43
1024	174	87	58
2048	234	117	78
4096	313	157	105
8192	417	209	139

Table 2.1: Сравнение на дължината на ключа в битове при ECC и HECC

ГЛАВА 3. ЛОКАЛНИ МЕТОДИ ЗА ОТКРИВАНЕ НА НЕТИПИЧНИ СТОЙНОСТИ

В трета глава на дисертационния труд са представени методи за откриване на локални нетипични стойности, които могат да бъдат приложени за поточни данни и позволяват изчисления при ограничение на използваната памет.

От разгледаните в първа глава методи за откриване на нетипични стойности са избрани тези, базирани на разстояние, при които оценката за нетипичност (отклонение) се определя на базата на най-близки съседи в обработваните данни. Това прави методите базирани на разстояние приложими в случаи когато предварително не е известно разпределението на данните. Методите за откриване на нетипични стойности базирани на разстояние се категоризират като глобални и локални в зависимост от използвания подход за определяне на оценката за отклонение. Предимствата на подходите за локално откриване на нетипични стойности е способността им да откриват отклонения в набори от данни с нехомогенни плътности на разпределение.

3.1. Методи за откриване на локални нетипични стойности

- Метод базиран на локален фактор на нетипичност (Local Outlier Factor, LOF)

За определяне на нетипичните стойности се използва локален коефициент на отклонение, изчислен за всяка точка от данните *p* както следва:

$$LOF_k(p) = \frac{1}{k} \sum_{O \in N_{(p,k)}} \frac{lrd_k(o)}{lrd_k(p)}$$

където е $N_{(p,k)}$ е множеството от k най-близки съседа на *p*, а $lrdk(p)$ се изчислява чрез:

$$lrdk(p) = (\left(\frac{1}{k}\sum_{O\in N_{(p,k)}} reach\_dist_k\,(p,o)\right)^{-1}$$

$$reach\_dist(p,o) = max\{k\_distance(o), d(p,o)\}$$

С *d(p,o)* е означено Евклидовото разсатояние между *p* и *o*, а с *k_distance(o)* – разстоянието между точка *o* и k-тия най-близък съсед.

Предимства: Добра точност и приложимост за определяне на нетипични стойности за набори от данни с нехомогенна плътност.

Недостатъци: Въпреки, че съществуват много различни версии и модификации на LOF, алгоритъмът не е приложим за определяне на локални отклонения в поточни данни.

- Инкрементален LOF метод (iLOF)

При метода LOF се изисква целия набор от данни за изчисляване на локалния фактор на отклонение за всяка точка от данните, докато при метода iLOF се използва инкрементален подход, който изисква само част от данните за актуализиране на LOF стойностите. За всяка входяща точка се определят k най-близки съседи, изчислява се локалния коефициент на отклонение на базата на локалните коефициенти на най-близките съседи и се актуализират локалните фактори на съседните точки ако е необходимо.

Предимства: Определянето на локалния фактор на отклонение е инкрементално и изчислително ефективно.

Недостатъци: За определянето на локалния фактор на отклонение се изисква всички данни да са налични и да се съхраняват в паметта, което прави алгоритъма неприложим за изчисления в реално време при поточни данни.

- Метод с ефективно използване на памет Memory Efficient iLOF (MiLOF)

Методът MiLOF е модификация на инкременталния метод с локален фактор на отклонение, приложим за поточни данни. При MiLOF се прилага обобщаване на фактора на отклонение за подмножества и натрупване на история за вече обработените поточни данни. По този начин се преодоляват ограничения за налична и използвана памет и се постига по-добра изчислителна ефективност.

Методът MiLOF включва няколко стъпки за локално откриване на отклонения при достигане на границите на паметта: стъпка на обобщаване, с-средна стъпка, стъпка на сливане, ревизирана стъпка на вмъкване. За всяка входна точка от данни стойността на локалния фактор на отклонение LOF се изчислява като се използва iLOF. След като се достигне ограничението на използваната памет се изчислява обобщение на фактора на отклонение за първите *b*/2 точки и те се изтриват от паметта. Обобщението за изтритите точки е под формата на набор от *c* прототипни вектора. Ако съществува набор от обобщени прототипи от предишен времеви прозорец, двата набора от прототипи се обединяват, с което се определя обобщение на минали точки от данни. Алгоритъмът продължава докато достигне края на потока от данни. Броят на съхранявани в паметта данни за откриване на отклонения е не повече от m = b + c.

Предимства: Добра скалируемост и ефективност по отношение на използвана памет

Недостатъци: Резултатите от прилагането на алгориртъма зависят от броя най-близки съседи, използвани за оценка на плътността.

- Метод с интеграл на локална корелация Local Correlation Integral (LOCI)

Методът LOCI използва коефициент MDEF (Multi-Granularity Deviation Factor), който позволява постигане на независимост при откриване на нетипични стойности от локални вариации на плътността в пространството на характеристиките, така че да бъдат определени както изолирани отклонения, така и отдалечени клъстери.

Коефициентът MDEF за точка p_i от входния поток данни оценява относителното отклонение на локалната плътност на съседство от средната плътност на локална околност с радиус r:

$$MDEF(\ p_i, r, \alpha\ ) = \frac{\mathrm{n'(p_i,r,\alpha)-n(p_i,\alpha r)}}{\mathrm{n\prime(p_i,\alpha,r)}} = 1 - \frac{\mathrm{n(p_i,\alpha r)}}{\mathrm{n\prime(p_i,\alpha,r)}}$$

където $n(p_i, r)$ е брой съседни точки за p_i в локална околност с радиус r, $\mathrm{n'}(pi, \mathrm{r}, \alpha)$ е средна стойност на $n(p, \alpha r)$ за множеството съседни точки на p_i в локална околност с радиус r:

$$\mathrm{n'}(pi, \mathrm{r}, \alpha) \equiv \frac{\sum_{p \varepsilon N(P_i, r)} n(p, \alpha \mathrm{r})}{n(p_i, r)}$$

С $\sigma_{n\prime}(pi, r, \alpha)$ е означено стандартното отклонение на $n(p, \alpha r)$ за множеството съседни точки на p_i в локална околност с радиус αr:

$$\sigma n'(pi, r, \alpha) \equiv \sqrt{\frac{\sum_{p \varepsilon N(P_i, r)} \left(n(p, \alpha r) - n'(p_i, r, \alpha)\right)^2}{n(p_i, r)}}$$

За точки, чиято плътност на съседство съвпада със средната плътност на локалната околност стойността на MDEF близка до 0, докато за нетипичните данни стойността на MDEF е висока. Методът LOCI приема, че точка е нетипична когато:

$$MDEF_{(pi, r, \alpha)} > k_\sigma \sigma_{MDEF}(pi, r, \alpha) \text{ за } k_\sigma = 3\sigma_{MDEF},$$

където $\sigma_{MDEF}(pi, r, \alpha)$ е нормализиран MDEF коефициент:

$$\sigma_{\mathrm{MDEF}}\ (\mathrm{p_i}\ ,\ \mathrm{r},\ \alpha) = \frac{\sigma \mathrm{n\prime(p_i\ ,r,\alpha)}}{\mathrm{n\prime(p_i\ ,r,\alpha)}}$$

Предимства: Преодолява се зависимостта от входен параметър за броя на най-близките съседи.

Недостатъци: Няма механизъм за намиране на оптимална стойност на радиуса на локалната околност за определяне на отклонение. Стойността на радиуса може да бъде потребителски дефиниран входен параметър или да бъде определена с помощта на алгоритъм за оптимизация.

3.2. Изводи от трета глава

В резултат на направения сравнителен анализ на локалните методи за откриване на нетипични стойности могат да бъдат направени следните по-важни изводи:

- Методът LOF не позволява откриване на нетипични стойности в поточни данни;
- Методът iLOF изисква всички данни да се съхраняват в паметта и не е приложим за работа в реално време при ограничения на наличната памет;
- Методът MiLOF позволява откриване на нетипични стойности в поточни данни, но определянето на отклонения зависи от потребителски дефиниран входен параметър;
- Методът LOCI премахва зависимостта от броя на най-близките съседи, но не предлага механизъм за намиране на оптимална стойност на радиус на ликална околност.

Модификация на метода LOCI с използване на оптимизационен алгоритъм за определяне на радиус на локалната област на съседство може да осигури ефективен подход за откриване на нетипични стойности при поточни данни.

ГЛАВА 4. Подход за криптиране, базиран на HECC

В тази глава се проучват различни възможни атаки на IoT системата заедно с различни техники и решения, които могат да направят IoT устройството сигурно и ефективно. Лекотата на IoT устройствата и проблемите с намаляването на ефективността и сигурността на тези устройства беше мотивация за проектиране на алгоритъм, който ще намали изчислителните разходи на устройството и ще увеличи неговата ефективност, като същевременно запази същото ниво на сигурност в сравнение с други алгоритми като ECC. Тук сме внедрили подхода за шифроване, базиран на HECC. Резултатите показват, че този подход е подходящ за приложение в IoT устройства с ограничени ресурси.

В предложения подход сме приложили хиперелиптична крива (HEEC) за генериране на ключове, като се има предвид факта, че такъв подход е по-подходящ за леки устройства поради по-малкия размер на ключа. Внедрихме подхода за шифроване на знаци, където цифровият подпис и криптирането трябва да са възможни в една логическа стъпка. Чрез прилагане на HEEC-базирано кодиране, постигнахме значително подобрение в сигурността и ефективността на устройствата с ограничени ресурси в IoT.

Обикновено в метода за шифроване на подателя изпращачът трябва да изпълни следното, преди да изпрати съобщение:

1. Използва техника за цифров подпис (DS) за подписване на съобщение.

2. Използва алгоритъм за криптиране на частен ключ и произволно определен ключ за шифроване на съобщение, шифрова съобщението и подписа.

3. Използва публичния ключ на приемника, шифрова ключа за криптиране на произволни съобщения.

4. Следва стъпки 1–3, за да изпрати съобщението.

Това е Signature-then-encryption метод. Най-големият недостатък на тази стратегия е, че цифровото подписване и последващо криптиране на комуникация отнема допълнителни цикли на процесора и раздува съобщението, като добавя допълнителни битове. В резултат на това дешифрирането и валидирането на съобщението при получателя отнема значително количество ресурси за обработка. В резултат на това разходите за подписване и криптиране на съобщение на практика представляват сумата от цените както на цифровите подписи, така и на криптирането с публичен ключ.

Традиционното решение е криптирането на предадените съобщения с помощта на криптосистеми с публичен ключ. Тъй като съобщенията се предават без каквато и да е физическа връзка в WSN, е лесно за противник да прихване, модифицира или изфабрикува съобщенията, преди да стигнат до местоназначението си. В резултат на това съобщенията трябва да бъдат подписани, преди да бъдат предадени. Криптографски примитив, наречен signcryption, който подписва и криптира едновременно в една логическа стъпка. Предимството на схемата за шифроване е, че нейните изчислителни разходи и режийни разходи за комуникация са по-ниски от

тези на традиционния метод за двуетапно подписване след криптиране. Повечето от съществуващите схеми за шифроване са еднородни, тоест те са или само базирани на PKI схеми за шифроване на публичен ключ или базирани на идентичност схеми за публично ключово кодиране. Тези хомогенни схеми за шифроване обаче не се представят добре за хетерогенни мрежови системи

„Signcryption е нова парадигма в криптографията с публичен ключ, която едновременно изпълнява както функциите на цифровия подпис, така и криптирането на публичния ключ в една логично стъпка и със значително по-ниска цена от тази, изисквана от традиционния„ подпис, последван от криптиране.

Въз основа на проблема с дискретния логаритъм, Signcryption струва 58% по-малко средно време за изчисление и 70% по-малко при разширяване на съобщението, отколкото кодирането след подписване.

Забелязва се, че използването на хипер елиптична крива с род 2 е по-малко от алгоритъма за криптография на кривата на елиптичната крива. Аритметиката на операциите става все по-сложна с увеличаването на рода. Но HECC осигурява същото ниво на сигурност с по-къси ключове и също така размерът на операнда му е малък, става по-подходящ за IoT устройства. Приложения като електронната търговия се нуждаят от леки алгоритми с по-висока сигурност за по-бързи транзакции. Резултат от сравненията ECC и HECC са дадени в таблица 2.1, която показва, че използването на HECC може да бъде добър вариант за увеличаване на ефективността на устройствата с ограничени ресурси в IoT. Изчислителните разходи за криптографски механизъм за HECC са по-ниски от ECC. Сравнението на ключовите размери на ECC и HECC в битове е показано в таблица 2.1.

HEEC от род $g > 1$ е крива, дадена от уравнение

$$y^2 + h(x)y = f(x) \qquad (4.1)$$

тук f (x) е полином на степен $n = 2g + 1 > 4$ или с $n = (2g + 2) > 4$различни корени и h(x) е полином на степен $< g + 2$ (ако характеристиката на полето не е равна на 2, можем да вземем $h(x) = 0$.

Граф $C: y^2 = f(x)$

Където $f(x) = x^5 - 2x^4 - 7x^3 + 8x^2 + 12x$

HECC е асиметричен тип криптографска техника с публичен ключ, при която се включва процес на генериране на ключове за частни и публични ключове. Всеки член в процеса има двойки частни публични ключове, където частният ключ се използва за дешифриране и генериране на цифров подпис, а публичният ключ се използва за криптиране и проверка на подписа.

Криптирането на знаци, базирано на хиперелиптична крива, следва криптография с публичен ключ за криптография за предаване на съобщения и изисква един алгоритъм за криптиране и алгоритъм за цифров подпис. Въз основа на задачата за дискретен логаритъм на хиперелиптичната крива (HECDLP) $PU = PR.G$ се нарича дискретен логаритмичен проблем на хиперелиптичната крива. Генераторът на частни ключове генерира ключовете за сензорно устройство и хост устройство. Разпределението на този ключ, т.е. $PR_{sensor}, PU_{sensor}, PR_{host}, PU_{host}$ се извършва по сигурен начин във фазата на инициализация. Когато тези ключове се

споделят сигурно, устройствата съхраняват своите частни ключове и са публичните ключове един с друг. Фиг. 13 показва схемата на подхода за шифроване и отписване.

HECDSA се формира чрез криптиране на знаци, където хиперелиптичната крива и цифровият подпис се извършват в една логическа стъпка. Тази стъпка е много важна стъпка, при която получаваме намалено изчислително време в сравнение с подхода и подхода на криптиране. Той осигурява същото ниво на сигурност като ECC. HECDSA е резултатът от техниката за криптиране.

HEEC над крайното поле Fp се обозначава с $E(Fp)$ с базова точка $G \in Fp$ от порядъка q, където G се взема безразборно от набор от точки на $E(Fp)$. Параметърът P е просто число, идентифициращо крайното поле Fp. Частните ключове се генерират чрез избор на число от множеството на голямо просто число. Три параметъра, необходими за шифроване на знаци:

$PU = PR \cdot G$ (Където PU е публичен ключ и PR частен ключ)

Цифров подпис (HECDSA)

Шифроване (AES)

Двойките ключове за сензорна единица и хост единица се дават съответно от PR_{sensor}, PU_{sensor} $PR_{,host}$ PU_{host}. В алгоритъма за шифроване избираме случайната променлива $P \in (1, 2, \dots, q-1)$

$$k1 = \text{hash}(P * G) \quad (4.2)$$

$$k2 = \text{hash}(P * PU_{host}) \quad (4.3)$$

$$c = \text{Encryptk2}(\text{data frame}) \quad (4.4)$$

$$r = \text{hash}(c, k1) \quad (4.5)$$

$$s = \frac{P}{(r+PR_{sensor})} \bmod q \quad (4.6)$$

$$R = r \cdot G \quad (4.7)$$

Следователно изходният сигнал за шифроване се дава от (c, R, s). След това съобщението с криптиран знак се прехвърля към хост устройството, където се извършва дезакриптиране. Сензорното устройство удостоверява зашифрованите данни чрез публичния си ключ и потвърждава автентичността му, ако $r \cdot G = R$.

Алгоритъм за декриптиране

Деактивирането на шифроването се извършва, когато съобщението с шифроване се получи на хост устройството

$$k1 = \text{hash}\big(s(R + PU_{sensor})\big) \quad (4.8)$$

$$r = \text{hash}(c, k1) \quad (4.9)$$

$$k2 = \text{hash}(PR_{host}(s(R + PU_{sensor}))) \quad (4.10)$$

$$\text{data frame} = \text{Decryptk2}\ (c) \qquad (4.11)$$

$$r.G = R \qquad (4.11)$$

За да се извърши демонстрацията, беше създадена настройка, където беше избрана Arduino Uno, която е свързана с нейните библиотеки, наречени Arduino pack. Arduino е платка за микроконтролер с отворен код, която създава среда, в която сензорният блок е в състояние да прехвърля рамки с данни към хост устройството, т.е. мобилно приложение. Arduino IDE, т.е.интегрираната среда за разработка е междуетапно приложение, например направено от C и C ++. Използва се за създаване и преместване на различни задачи към Arduino. Използването му зависи от езика C, който ангажиментите към момента са изпълнени, за да изпълнят ECC с изкривена Montgomery на Arduino Uno. Изходният код за Arduino IDE се предава под обществените лицензи. В нашата схема ние предварително зареждаме използваната хиперелиптична крива и нейните граници в паметта на устройството. Хиперелиптичната крива е подходяща за криптография за леки устройства в IoT. Всяка хиперелиптична крива не може да се използва. За наше вдъхновение трябва да ги накараме да се ориентират към тяхното семейство, искането за събиранията и тяхното поле на дефиниция. Смесването на HECC и DSA може да се справи с въпроса за проверка на почтеността на отчета и отпечатъка Id при електронни обстоятелства, когато е необходимо одобрение на id.

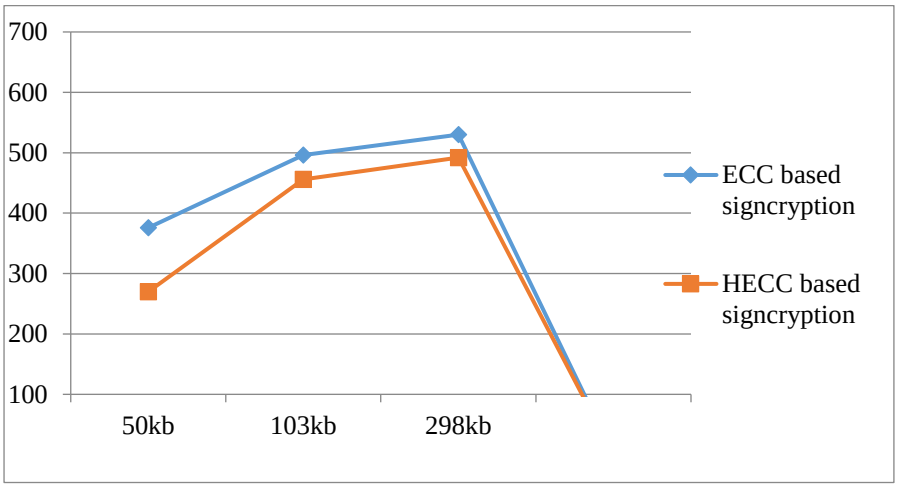
Данните за устройствата в ръка са ATmega328P микроконтролер, тактова честота 16 MHz, 32kb памет, SRAM 2kb, флаш памет 32kb. Той изчислява изчислителното време на различните рамки от данни, получени в сензорния блок, показан в таблица 4.1. Рамките с данни се съхраняват в кодиране Base-32, за да се даде възможност за AES криптиране по време на процеса на шифроване. Двойките ключове HECC са по-малки по размер в сравнение с ECC и RSA. Шифроването на знаци въз основа на HECC установи, че е по-ефективно със същото ниво на сигурност при по-малки размери на ключовете. Следователно изчислителното време, необходимо за HECC базирано кодиране на получената рамка на данни, е по-малко от ECC базирано кодиране. Операциите за събиране и умножение в HECC изискват по-малко време в сравнение с ECC. Докато демонстрираме, ние взимаме рамки за данни с различни размери и наблюдаваме изчислителните разходи за HECC базирана сигнализация и ECC базирана сигнализация, както е показано в таблица 4.1.

Block size Kb	ECC based signcryption (ms)	HECC based signcryption (ms)
50	376	270
103	496	456
298	530	492

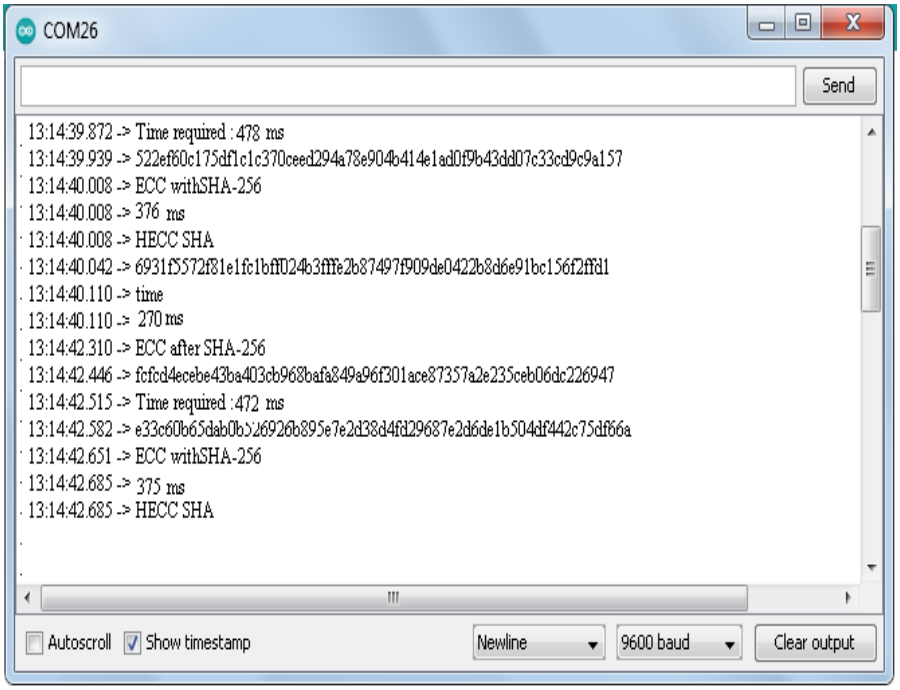
Табл 4.1: Време за изчисление в ms

Поради най-краткия размер на ключа и използването на цифров подпис и криптиране в една стъпка, базираното на HEEC криптиране има възможни фокусни

точки върху съществуващите произведения. Показано е, че едно и също ниво на сигурност може да бъде постигнато чрез HEEC, използвайки най-късата дължина на ключа, следователно изпълнението на HEEC, съставено подписване по отношение на рамките на данните, изисква по-малко изчислителни разходи, както е показано в таблица 4.1, където е дадено изчислително време в милисекунди. Дейностите по добавяне и умножаване на HEEC са най-досадните операции по мерки за криптиране и отписване. Независимо от това, струва си да се види, че тези части трябва да бъдат изпълнени само един път към началото на взаимодействието на шифроването и от този момент нататък, само операторът за криптиране или дешифриране влияе върху времето за изпълнение. Агентите за ускоряване на оборудването за хеш капацитет, AES и HEEC на сензорните устройства могат да подобрят изчислителната ефективност.



Фиг.15. Сравнителен анализ на HECC и ECC



Фиг.16. Резултати

Обща метрика за ефективност за леки криптографски алгоритми.

Общите показатели за производителност за всеки лек криптографски алгоритъм се дават от

Metric $(A^{\alpha}, T_B^{\beta}, E_B^{\lambda}, C_B^{\tau}, N_B^{\mu}) = \frac{A^{\alpha}, T_B^{\beta}, E_B^{\lambda}, C_B^{\tau}}{N_B^{\mu}}$,

където, A е площта; TB времето за криптиране на един блок; E е енергията; CB е броят на циклите за криптиране на един блок; NB е размерът на блока; α β λ τ и μ са коефициенти на мощност. Чрез използването на тази метрика и стойностите на коефициента. Следователно, като се вземе предвид изчислителното време за 50kb блок според HEEC базиран подход за шифроване е 270ms. Можем да изчислим производителността на всеки софтуер или хардуерна система като

Пропускателна способност = $\frac{T_B^{\beta} C_B^{\tau}}{N_B^{\mu}} = \frac{270^{-1}}{50^{-1}}$ = 0,18 блок / ms

По този начин, познавайки производителността на алгоритмите, можем да определим ефективността на алгоритмите и да проверим възможността за използването му, като се има предвид приложението.

Тази глава има един основен принос, свързан с проектирането на ефективна система, използваща HECC базирана сигнализация.

Криптирането на знаци, базирано на криптография на хиперелиптична крива, изисква един алгоритъм за криптиране и алгоритъм за цифров подпис. Въз основа на проблема с дискретен логаритъм на Hyper Elliptic Curve (HECDLP) се предлага подход за генериране на ключовете за сензорния блок и мобилния блок, след което разпределението на тези ключове (т.е. се извършва по сигурен начин във фазата на инициализация Следвайки устройствата съхраняват техните частни ключове и споделят публичните ключове един с друг.

В предложената система се използва HEEC-базирано криптиране, за да се осигури информация, уловена от Sensing unit за случай, започнал наблюдение в IoT приложения. Първоначално разпознахме очакваните опасности за такива приложения и след това разгледахме избрани проблеми със сигурността. Предложеното шифроване на знаци, което се изпълнява на детекторния блок, дава противодействащи мерки на потенциалните опасности и дава възможност за легитимност на кодираните снимки на ненадеждни сензорни устройства, без да се договаря класификацията му. Резултатът показва, че HEEC подходът за шифроване е подходящ за устройства с ограничени ресурси, които обикновено се намират в IoT.

НАУЧНО-ПРИЛОЖНИ И ПРИЛОЖНИ ПРИНОСИ

Научно-приложни приноси:

1. Направено е подробно проучване и сравнителен анализ на леките криптографски алгоритми и техните проблеми със сигурността, като се взети предвид изискванията за сигурност на различни нива. В резултат на проучването, са идентифицирани основни изисквания за сигурност и ефективността им.

2. За да бъдат ефективни и сигурни за IoT устройства с ниско ниво на изчислителната мощност се изискват и по-малко ресурси. Установено е, че в такива случаи за сигурен трансфер на данни в IoT сценарии едно подходящо решение е прилагане на протокол за нулево знание в комбинация с криптография с хиперелиптична крива.

3. Извършен е анализ на различни налични хиперелиптични криви за да се установи коя крива е подходяща за ограничените от ресурси IoT приложения. Предложен е усъвършенстван сигурен и ефективен протокол, използващ HECC, за осигуряване на сигурността на IoT устройства, който може да бъде използван за валидиране и легитимиране на потребителите, когато те имат достъп до устройството от разстояние.

4. Шифроването на знаци въз основа на криптография с хиперелиптична крива изисква криптиращ алгоритъм и алгоритъм за цифров подпис. Въз основа на дискретната хиперелиптична логаритмична задача (HECDLP) се предлага подход за генериране на ключове за сензорния блок и мобилния блок, след което е направено и разпределението на тези ключове по сигурен начин във фазата на инициализация. Устройствата съхраняват своите частни ключове и споделяйте публичните ключове едно с друго.

СПИСЪК НА ПУБЛИКАЦИИТЕ ПО ДИСЕРТАЦИОННИЯ ТРУД

IV. СПИСЪК С ПУБЛИКАЦИИ ПО ТЕМАТА НА ДИСЕРТАЦИОННИЯ ТРУД

[A1] Santosh Pandurang Jadhav “Towards Light Weight Cryptography Schemes for Resource Constrained Devices in IoT” Journal of Mobile Multimedia, Vol. 15_1&2, 91–110. doi: 10.13052/jmm1550-4646.15125 c 2020 River Publishers.

[A2] Santosh P. Jadhav, Georgi Balabanov, Vladmir Poulkov. “Hyper elliptic curve based signcryption scheme ,” Information Technology in Industry. ISSN (Print): 2204-0595 ISSN (Online): 2203-1731.

[A3] Santosh P. Jadhav, Georgi Balabanov Vladimir Poulkov and Javed R. Shaikh “Enhancing the Security and Efficiency of Resource Constrained Devices in IoT,” 2020 International Conference on Industry 4.0 Technology (I4Tech) Vishwakarma Institute of Technology, Pune, India. Feb 13-15, 2020

[A4] Santosh P. Jadhav, Georgi Balabanov, Vladmir Poulkov Technique for Enhancing the efficiency and security of lightweight IoT devices 5th International Conference on Advances in Computing and Data Sciences (ICACDS) 2021 ICACDS/2021/Author/080

SUMMARY

Enhancing Security and Efficiency of Resource Constrained Devices in IoT.

Jadhav Santosh Pandurang

Rapid increment of IoT has approached the IoT business to reinforce the safeguards of IoT devices using cryptography. Different endeavors are taken by the analysts to ensure the information generated by IoT devices and the more extensive security of IoT networks structure part of which is the new "lightweight cryptography" activity. This requests the formation of new calculations and methods that can work away at basic, low-power circuits. The test is that numerous IoT devices specifically utilize irrelevant electrical force, and hardware that is undeniably more restricted than even the chips found in basic telephones, however regular encryption strategies normally request a larger number of assets than that. Along these lines, at last the objective of the scientist ought to be to think of lightweight encryption guidelines that advantage the whole commercial market. Viable norms should bring a very much characterized arrangement that applies to a wide class of circumstances. Getting the IoT at straightforward devices level is a goal, along these lines inability to do so would make a massive attack surface that would be practically difficult to fix sometime later.

Different areas of IoT application generate very valuable data, which may be health related data or money transaction data, that are useful for various applications and decisions. Data can be confidential and sensitive and must be taken care of. Because of its rapid growth in IoT, it had become more prone to various cyber-attacks. Hence, it becomes of great importance to look into security measures, taking care that it should not affect the efficiency of IoT devices. Because of the enormous assortment and heterogeneity of IoT devices and the security goals of the applications utilizing them, lightweight cryptographic algorithms for the IoT have demonstrated challenging tasks to be solved. Challenges exist, both regarding giving satisfactory security and according to the effect on device execution, requiring critical tradeoffs versus the network safety levels we are utilizing. Such tradeoffs may limit the kind of utilizations that we can apply IoT devices in the long term, at any rate until a protected lightweight arrangement is created.

In this thesis, the design and implementation of various techniques and algorithms which found to be effective in enhancing the security and efficiency of resource constrained devices are implemented. Asymmetric algorithm hyper elliptic curve cryptography (HECC) along with zero knowledge protocol (ZKP) for authentication together with signcryption technique is used to reduce the computation cost of the cryptographic process. This work primarily focuses on enhancing the security and efficiency of tiny lightweight devices in IoT which are also called as “resource constrained” devices because they have low computational power.

The title of this thesis is defined as “Enhancing the security and efficiency of resource constrained devices in IoT”, with the goal defined as to design and develop secure, efficient, lightweight and reliable authentication technique that could be implemented in resource-constrained applications having high-security requirements and to design of secure and trustworthy authorization technique to protect the IoT devices from the various attacks. To fulfill the above stated goal various protocols and techniques are developed which provide the secure and efficient environment to the IoT system by proving the authentication, authorization and integrity services during the sensitive and highly confidential data transmission.

From the literature it is clear that, many researchers had concentrated on the lightweightness of the IoT devices and therefore many symmetric and asymmetric algorithms are written in order to suit the tiny devices an improving the efficiency of these resource constrained kind of devices. Various algorithms and its strength are discussed here. IoT devices are increasing day by day and as effect data transmission is reached at huge level. Therefore securing this data transmission along with making the system efficient is focused. After studying various algorithms we found HCC an asymmetric algorithm which is counterpart of ECC most suitable for tiny IoT devices.

In chapter one was shown the comparison between HECC and ECC and come to conclusion that HECC with genus 2 is an appropriate choice in implementation for making resource constrained devices efficient as the computational cost of HECC found to be lesser then ECC. Also, performance matrix is demonstrated in order to calculate the efficiency of the algorithm implemented.

HECC description and implementation is given in Chapter 2 the comparative result analysis of HECC with ECC is shown the table the various sizes block are taken as input and the computational time of them is calculated here it was noticed that the computational time for HECC encryption and decryption is lesser then ECC, which shows that the using HECC based cryptography for lightweight devices in IoT is more suitable then ECC.

Zero knowledge protocol (ZKP) along with HECC is implemented in Chapter 3. The advantages of ZKP which found to be one of the most secure authentication protocol is used for secure transmission of data. This combination of ZKP and HECC provides secure and efficient transactions. The tabular result shows that HECC with ZKP is more efficient and secure then ECC with ZKP, thus providing higher level of security for resource constrained IoT devices.

HECC based signcryption approach is implemented in Chapter 4. Signcryption can one of the efficient techniques to reduce the computational cost of any algorithm and thus found suitable in lightweight devices in IoT. The HECC based signcryption is implemented and the results shows that the computational time for HECC based signcryption is less than ECC based signcryption algorithm.