УДК 004.056.55 **DOI 10.52167/1609-1817-2024-132-3-246-257**

Ж.Е. Сейтбатталов[1], Ш.Ж. Канбаева[2], М.И. Бекенов[1],
О.К. Тасмагамбетов[1], Г.А. Тулешева[3]
[1]Евразийский Национальный Университет им. Л.Н. Гумилева, Астана, Казахстан
[2]АО «Государственная техническая служба», Алматы, Казахстан
[3]Satbayev University, Алматы, Казахстан
E -mail: sbtl.jeks@gmail.com

ИНТЕЛЛЕКТУАЛЬНЫЕ АЛГОРИТМЫ НИЗКОРЕСУРСНОЙ КРИПТОГРАФИИ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ГРАНИЧНЫХ ВЫЧИСЛЕНИЙ И ИНТЕРНЕТА ВЕЩЕЙ (IOT)

Аннотация. В статье представлено современное развитие Интернета вещей (IoT) и технологии граничных вычислений, а также рассмотрены способы обеспечения безопасности информации и протоколов взаимодействия между различными уровнями IoT сетей. Существующие методы обеспечения безопасности предъявляют высокие требования к вычислительным и энергетическим ресурсам IoT-устройств. Для решения этих проблем необходимо провести анализ следующих параметров IoT-устройства и граничных узлов на базе нечеткой логики: размер данных; объем памяти; пропускную способность сети; вычислительную мощность и мощность батареи. В результате на основе анализа этих параметров была предложена интеллектуальная модель для выбора оптимального алгоритма взаимодействия между граничными узлами интернета вещей, оптимизирующий уровень потребления энергии и использования вычислительных ресурсов узла, а также повышающий уровень безопасности.

Ключевые слова. Интернет вещей (IoT), граничные узлы (edge nodes), улучшенный гибридный легковесный алгоритм (EHLA), низкоресурсная криптография, протокол, алгоритмы шифрования, безопасность информации.

Введение.

«Интернет вещей» – совокупность разнообразных приборов, датчиков, устройств, используемых ранее локально и автономно, объединённых в сеть посредством любых доступных каналов связи, использующих различные протоколы взаимодействия между собой и единственный протокол доступа к глобальной сети.

Концепция Интернета вещей (Internet of Things, IoT) предусматривает постоянное наличие связи между всевозможными устройствами, наделяя все аспекты повседневной жизни преимуществами, которые дает Сеть.

IoT - устройства имеют единый протокол взаимодействия, согласно которому любой узел сети равноправен в предоставлении своих сервисов. Каждый узел сети интернет-вещей предоставляет свой сервис, оказывая некую услугу поставки данных. В то же время узел такой сети может принимать команды от любого другого узла.

За последнее десятилетие наблюдался обвальный рост количества подключаемых к сети устройств, и, судя по статистике: в феврале 2017 года количество перечисленных агентов составило около 10 миллиардов устройств. Некоторые устройства хранят очень важную и приватную информацию. Например, система дверных замков в квартире хранит номер кода блокировки. Массив подобных устройств, несмотря на среднюю мощность, не может быть оставлен без защиты [1]. Это подтверждается значительными последствиями в результате пренебрежения безопасностью интернет вещей [2],[3]. Примером могут служить атаки ботнетов brickerbot, Amnesia и Mirai в средствах массовой информации,

которые объединили сотни тысяч устройств, которые впоследствии использовались для проведения массовых DDoS-атак.

Рисунок 1 - Функциональная схема IoT-устройства

При этом ожидается постоянное совершенствование устройств, услуг и приложений, и многие организации, пытаясь в большинстве случаев воспользоваться преимуществами бизнеса, не проявляют осторожности в предотвращении угроз безопасности IoT-устройства. По этой причине при развертывании Интернета вещей предприятия сталкиваются с уникальными проблемами обеспечения безопасности, конфиденциальности и соответствия требованиям. Однако, стоит отметить, что частично проблему безопасности решает применение парадигмы граничных вычислений, исключая взаимодействие IoT-устройства с облаком. Технология граничных вычислений в отличии от облачных вычислений позволяет устройству принять решение на месте генерации данных и не отправлять необработанные данные по интернет сети в облако, тем самым обеспечивая автономность IoT-устройства.

Если традиционная информационная безопасность вращается вокруг программного обеспечения и подходов к его реализации, безопасность для Интернета вещей на уровень сложнее, так как он объединяет виртуальный мир с физическим. Широкий диапазон сценариев работы и обслуживания в сфере Интернета вещей зависит от возможности подключения всех необходимых устройств. Только тогда пользователи и службы смогут взаимодействовать, выполнять вход в систему, устранять неполадки, а также отправлять или получать данные с помощью устройств.

Из этого возникает явная задача обеспечения безопасности и приватности данных, передаваемых IoT-устройствами. К сожалению, спроектировать совершенно безопасную IoT систему очень непростая задача. Во-первых, потому что IoT системы очень разнородные, они состоят из различных устройств, которые имеют разные операционные системы, аппаратные средства, используют различные протоколы. Во-вторых, системы очень масштабны, они могут быть, как в пределах одной квартиры, так и распространятся на города и даже страны. В-третьих, многие IoT-устройства имеют ограниченные ресурсы, как память, вычислительную мощность и емкость аккумулятора и др.

Материалы и методы.

Хотя устройства в мире Интернета вещей могут казаться слишком незначительными или узкоспециализированными, чтобы представлять опасность, есть риск, что злоумышленники получат контроль над подключенными в сеть компьютерами общего назначения. Это создаст проблемы, уже выходящие за рамки безопасности Интернета вещей и парадигмы граничных вычислений. После получения контроля злоумышленники могут украсть данные, прекратить работу служб или совершить любое

другое киберпреступление, как совершили бы его с помощью компьютера. Атаки со взломом инфраструктуры Интернета вещей приводят к ущербу.

При разработке нового метода шифрования данных необходимо провести анализ существующих методов шифрования и учесть фактор ограниченности вычислительных ресурсов IoT-устройств.

Прежде чем определить алгоритм, который будет разработан для обеспечения безопасности и защиты от атаки, рассмотрим архитектуру IoT, разделяя ее на логические уровни, которые могут взаимодействовать как вертикально, так и горизонтально. Все уровни архитектуры IoT сети неразрывно связаны с обеспечением безопасности в процессе передачи данных.

Таблица 1 – Уровни архитектуры IoT

<table>
<tr><td colspan="3">Архитектура IoT</td></tr>
<tr><td>Уровень приложений</td><td>Персонализированные приложения;
Область применения: медицина, транспорт, промышленность, быт, умный город.</td><td rowspan="4">Безопасность IoT</td></tr>
<tr><td>Уровень IoT облака или вычислительного ядра</td><td>Обработка и хранение Big Data;
Управления устройствами;
Применение алгоритмов машинного обучения (ML).</td></tr>
<tr><td>Уровень коммуникаций</td><td>Передача данных;
Коммуникационные протоколы;
Различные сети.</td></tr>
<tr><td>Уровень IoT-устройств или граничного узла</td><td>Сенсоры, датчики, RFID коммуникации.</td></tr>
</table>

Алгоритмы шифрования больше затрагивают уровень IoT-устройств, так как датчики, получают данные, которые нужно передать. И в свою очередь алгоритмы шифрования решают такие проблемы как:

1) Конфиденциальность.
2) Целостность данных.
3) Подлинность сообщения.

Основные роли алгоритма низкоресурсной криптосистемы в обеспечении безопасности IoT и технологии граничных вычислений [4],[5]:

1) Защита конфиденциальности данных передаваемых и хранимых на IoT-устройствах. Они позволяют шифровать данные таким образом, чтобы только авторизованные устройства или пользователи могли их расшифровать.

2) Защита от подделки и аутентификация протоколы и алгоритмы цифровой подписи на основе низкоресурсной криптографии используются для проверки подлинности устройств и данных, передаваемых через IoT сеть. Это помогает предотвратить атаки по типу подделок, когда злоумышленник пытается подменить устройство или данные.

3) Защита от перехвата и модификации данных обеспечивают защиту от атак, направленных на перехват и модификацию данных, передаваемых между устройствами IoT или к управляющим серверам. Это помогает гарантировать целостность данных и предотвращать несанкционированные изменения.

4) Энергоэффективность, учитывая ограниченные ресурсы IoT-устройств, алгоритмы низкоресурсной криптографии оптимизированы для минимального потребления энергии и вычислительных ресурсов. Они позволяют достигать безопасности при минимальной нагрузке на устройства, что особенно важно для батарейных или энергонезависимых устройств.

5) Алгоритмы низкоресурсной криптографии включают в себя механизмы для безопасного управления ключами и их обмена между IoT-устройствами. Это обеспечивает конфиденциальность и целостность данных во время их передачи и хранения.

6) Защита от различных видов атак: алгоритмы низкоресурсной криптографии разработаны с учетом специфических угроз, с которыми сталкиваются IoT-устройства, таких как атаки с использованием боковых каналов или атаки, основанные на физических характеристиках устройств. Боковые каналы или атаки, основанные на физических характеристиках устройств, являются методами атаки, при которых злоумышленник использует физические характеристики устройства, такие как электромагнитные излучения, потребление энергии, электрический шум и другие, для извлечения конфиденциальной информации или выполнения нежелательных действий.

Есть два способа реализовать легковесный алгоритм шифрования через симметричный или асимметричный ключ шифрования данных.

В процессе симметричного шифрования отправитель и получатель совместно используют общий ключ, передающийся по зашифрованному каналу как для шифрования, так и для дешифрования. Симметричная криптография больше подходит для IoT приложений из-за оперативности процесса шифрования, поскольку в основе лежат операции XOR («или») и перестановки. Скорость обработки выше, и они не используют много ресурсов.

Таблица 2 – Характеристика легковесных симметричных алгоритмов шифрования и вероятные сценарии атак

Легковесные симметричные алгоритмы						
Симметричный алгоритм	**Длина кода**	**Структура построения шифра**	**Количество раундов**	**Размер ключа**	**Размер блока**	**Возможная атака**
AES	2606	SPN	10	128	128	Атака посредника
HEIGHT	5672	GFS	32	128	64	Атака с насыщением
TEA	1140	Feistel	32	128	64	Атака на связанных ключах
PRESENT	936	SPN	32	80	64	Дифференциальная атака
RC5	Не фиксированно	ARX	20	16	32	Дифференциальная атака

Путем работы над такими параметрами, как выбор блочного или потокового шифра, размера ключа, размера блока, выбор структуры построения блочного шифра и количества раундов получаются легкие симметричные алгоритмы.

Асимметричные методы шифрования данных меньше подходит для реализации легковесных алгоритмов шифрования. Однако, их также стоит рассмотреть. Легковесные асимметричные алгоритмы сложны с точки зрения работы и неэффективны по времени.

Но при этом совсем недавно упор сместился в сторону криптографии с асимметричным ключом в области легковесной криптографии.

В таблицах ниже показаны основные легковесные асимметричные алгоритмы шифрования и указаны их характеристики, а также типы атак, к которым они наиболее уязвимы.

Таблица 3 – Характеристика легковесных асимметричных алгоритмов шифрования и вероятные сценарии атак

Легковесные асимметричные алгоритмы			
Асимметричный алгоритм	**Размер ключа**	**Длина кода**	**Возможная атака**
RSA	1024	900	Модульная атака
ECC	160	8838	Атака по времени

Таким образом, на основе анализа двух табличных данных формируется вопрос применения того или иного алгоритма шифрования для частного случая. Одним из таких оптимальных и уникальных способов анализа является HLA (Hybrid Lightweight Algorithm). Он позволяет учесть различные ресурсы устройств.

На рисунке 2 указана блок-схема, в которой входом является IoT-устройство, а в выходных данных предлагается подходящая схема шифрования для этого устройства [6]. Этот подход использует следующие четыре параметра конкретного устройства в качестве входных данных: размер данных (РД), объем памяти (ОП), вычислительную мощность (ВМ) и мощность батареи (МБ). Пороговое значение каждого параметра можно рассчитать по определенному алгоритму [7],[8] или зная характеристики устройства.

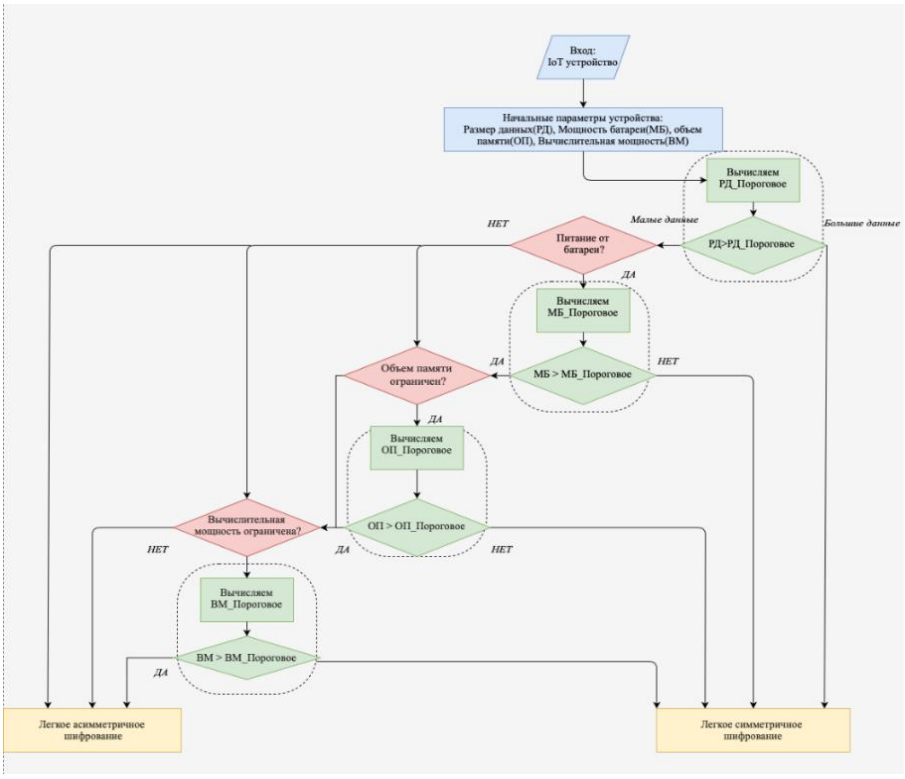


Рисунок 2 – Блок-схема гибридного легковесного алгоритма (Hybrid Lightweight Algorithm, HLA)

Во-первых, HLA анализирует размер данных, передаваемых по сети. Сначала учитывается размер данных, а затем подбираем криптографический алгоритм. Если размер данных превышает пороговое значение, они считаются большими данными и на основании существующих исследований [9] рекомендуется для легкого симметричного шифрования, в противном случае - для последующей фазы анализа.

Так далее согласно схеме, мы анализируем остальные параметры конкретного устройства, и в конце принимаем решение использовать симметричный или асимметричный алгоритм.

Разработанный протокол алгоритмов позволяет осуществить безопасную аутентификацию устройства, подтвердить его наличие в сети и осуществить безопасный обмен информации с устройством.

Протокол использует следующие средства для выполнения данных задач:

- уникальные метки устройств;
- магические числа;
- шифрование каналов связи с использованием сессионных ключей.

При разработке протокола учитываются некоторые важные параметры способа защиты, такие как: минимальные требования к мощности контроллера и скорости передачи данных. Размер передаваемых пакетов в текущей версии минимизирован.

Для реализации улучшенной модели алгоритма HLA на базе нечеткой логики применялся язык и среда программирования MATLAB R2022b. На рисунке 3 представлена модель улучшенного гибридного легковесного алгоритма шифрования (Enhanced Hybrid Lightweight Algorithm, EHLA) с входными и выходными параметрами: размер данных; мощность батареи; объем памяти; вычислительная мощность; пропускная способность сети; симметричный и асимметричный ключ шифрования.

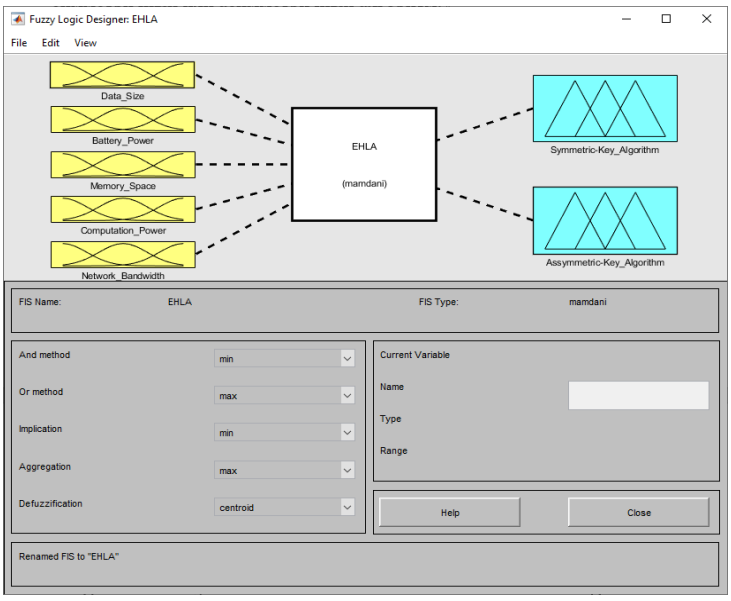


Рисунок 3 – Модель гибридного легковесного алгоритма шифрования в MATLAB

На рисунке 4 представлены графики принадлежности для размера данных, измеряемых в мегабайтах. В качестве лингвистических переменных введены: Low – небольшой размер данных; Medium – средний размер данных; High - большой размер данных. Функции принадлежности представлены в виде нормального распределения Гаусса.

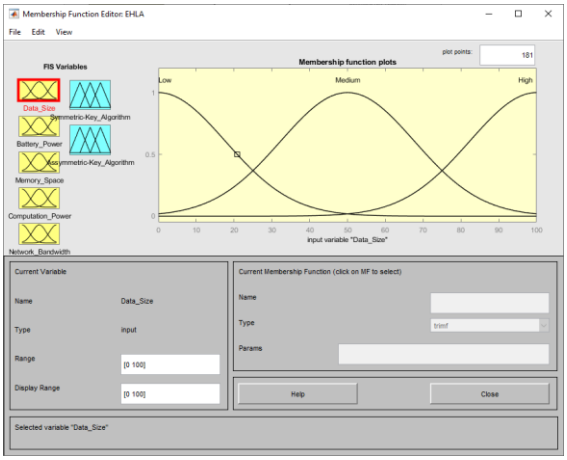
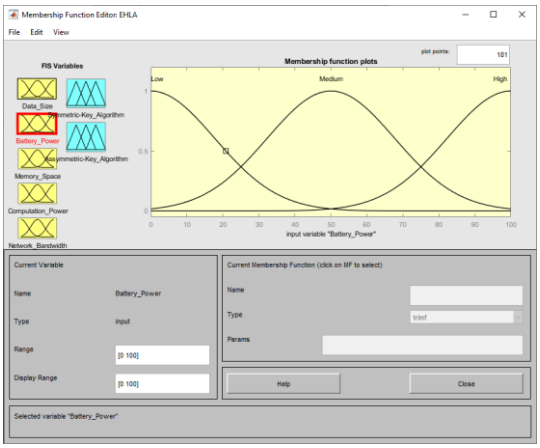
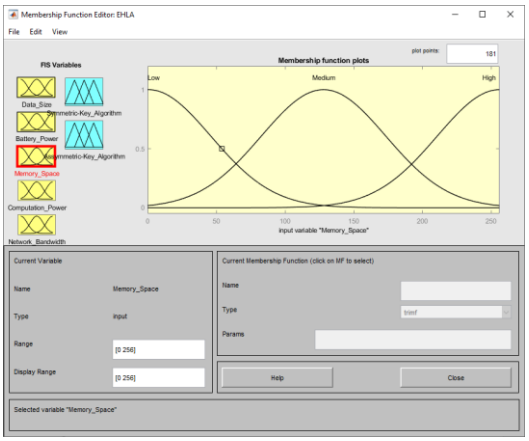


Рисунок 4 – Графики принадлежности для размера данных (РД)

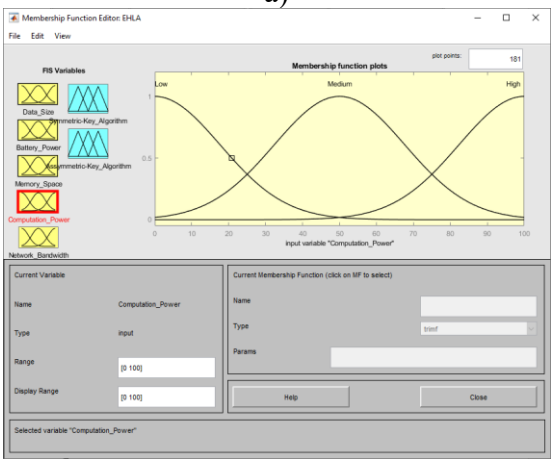
Таким же образом, на рисунке 5 представлены графики принадлежности для мощности батареи в процентах от всего объема, объема памяти в мегабайтах, вычислительная мощность в процентах от всего объема ресурсов и пропускная способность сети в мегабитах/секундах.



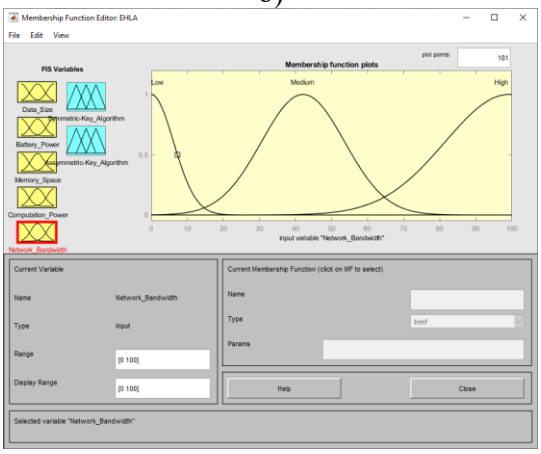
а)



б)



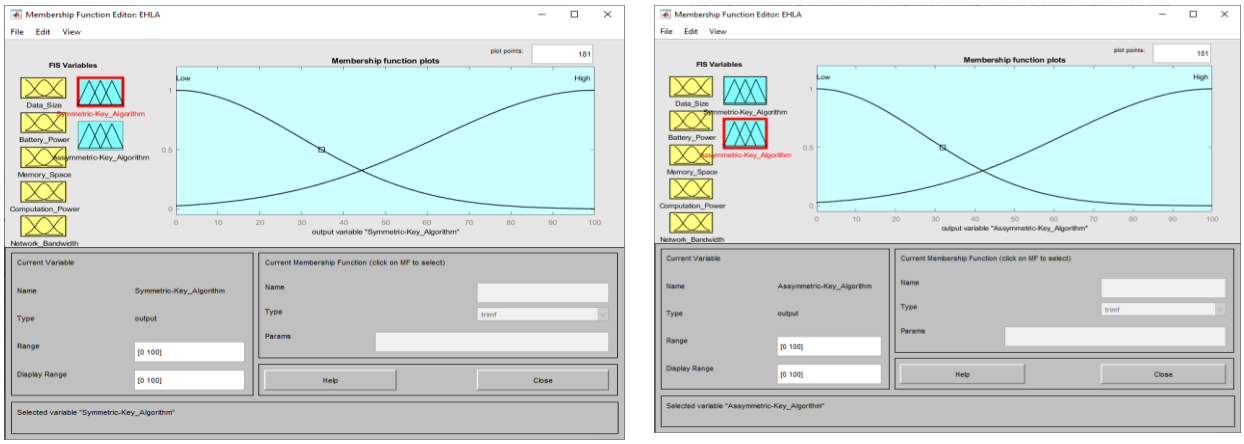
в)



г)

Рисунок 5 – Графики принадлежности для входных параметров: а) мощность батареи (МБ); б) объем памяти (ОП); в) вычислительная мощность (ВМ); г) пропускная способность сети (ПСС)

Для вероятности реализации алгоритма шифрования с асимметричным или симметричным ключом шифрования представлены в виде графиков принадлежности на рисунке 6.



а) б)

Рисунок 6 – Графики принадлежности для выходных параметров: а) алгоритм шифрования с симметричным ключом; б) алгоритм шифрования с асимметричным ключом

Для реализации модели была создана база правил, представленная на рисунке 7.

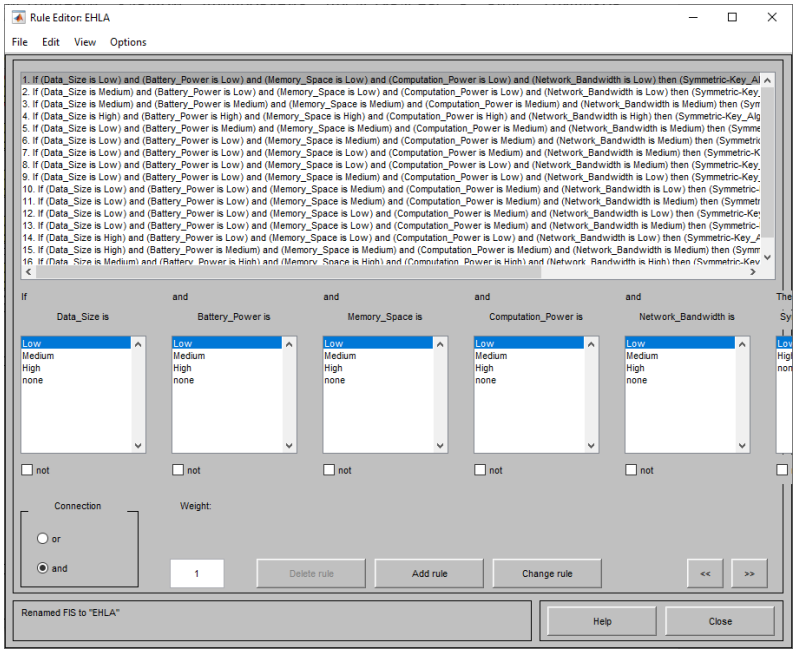


Рисунок 7 – База правил в MATLAB

Результаты и обсуждение

В результате пользователь может проверить вероятность выбора асимметричного или симметричного ключа шифрования для граничного узла и IoT-устройства. На рисунке 8 представлен частный случай с указанием РД=10 мегабайт; МБ = 20 %; ОП = 100 мегабайт; ВМ = 25 %; ПСС = 25 мегабит в секунду. Для данного случая, основываясь на базе правил с большей вероятностью (62.1%) является оптимальным асимметричный способ шифрования информации.

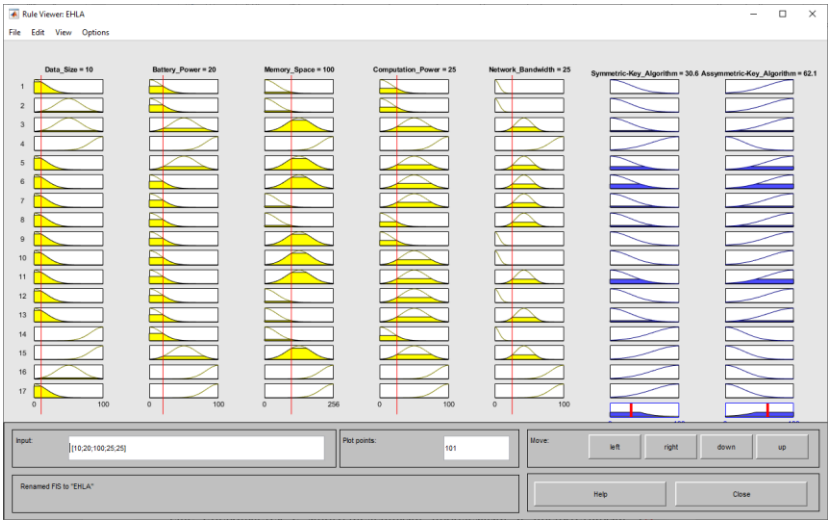
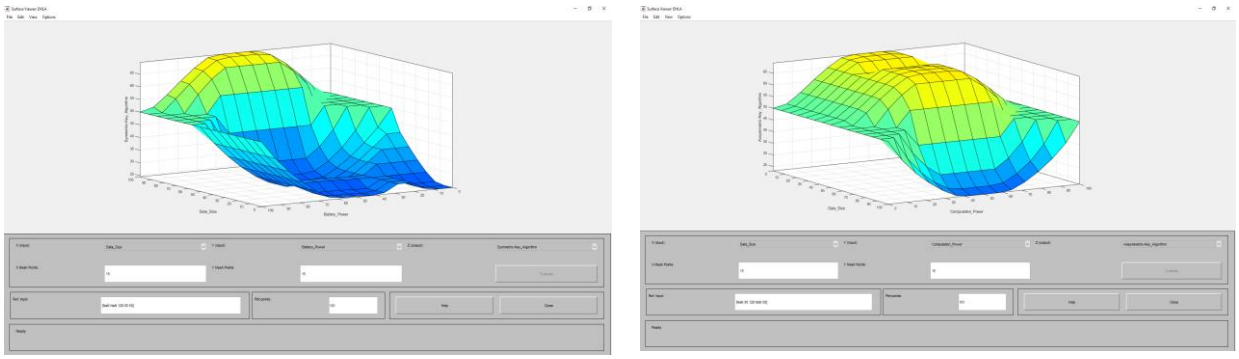


Рисунок 8 – Просмотр баз правил в MATLAB

Для рассмотрения результатов с широким диапазоном числовых показателей для входных параметров пользователь может просмотреть 3D-график в виде поверхности для вероятности выбора асссиметричного и симметричного алгоритма шифрования в зависимости от двух входных параметров (рисунок 9).



а) б)

Рисунок 9 – 3D-графики поверхности для: а) симметричного алгоритма шифрования; б) асимметричного алгоритма шифрования

На рисунке 9, а представлен 3D-график поверхности симметричного алгоритма шифрования с такими входными параметрами как ОП и МБ. Как показывает трехмерный график, рост ОП значительно увеличивает вероятность выбора симметричного алгоритма шифрования.

Рисунок 9, б иллюстрирует 3D-график поверхности ассимметричного алгоритма шифрования с такими входными параметрами как ОП и ВМ. Как видно из трехмерного графика, невысокие показатели ОП и ВМ увеличивают вероятность выбора ассимметричного алгоритма шифрования.

Заключение

Таким образом, алгоритмы низкоресурсной криптографии играют ключевую роль в обеспечении безопасности IoT, позволяя реализовывать криптографические методы защиты данных на устройствах с ограниченными ресурсами, сохраняя при этом их энергоэффективность.

Основным требованием исследования является обеспечение информационной безопасности соответствующего устройства IoT с использованием вышеуказанных методов шифрования. Количество устройств и их многообразие свидетельствуют о том, что к IoT-устройствам удобно применять симметричный легкий алгоритм шифрования, а его ограниченные факторы также являются необходимым методом защиты от различных атак, полного сохранения информативности. Просматривая таблицу типов атак, часто встречающихся в методе симметричного шифрования, мы обнаружили, что атаки на устройства IoT также происходят из этого типа. Это означает, что использование легкого симметричного метода шифрования будет удобным и продуктивным исследованием для защиты безопасности Интернета вещей.

В результате нами была предложена интеллектуальная модель для выбора оптимального алгоритма шифрования и взаимодействия между граничными узлами интернета вещей, оптимизирующий уровень потребления энергии и использования вычислительных ресурсов узла, а также повышающий уровень безопасности. Данная модель также может быть улучшена и расширена за счет добавления новых входных параметров для анализа с целью способствования принятия более оптимального решения.

В будущих исследованиях нами планируется реализация данной модели на базе IoT-устройства со снятием показании и результатами изменении криптографической стойкости системы.

Благодарность.

Данная работа выполнена при финансовой поддержке Комитета науки Министерства науки и высшего образования Республики Казахстан (ПЦФ № BR18574045).

ЛИТЕРАТУРА

[1] Облегченные алгоритмы шифрования - https://link.springer.com/article/10.1007/s12652-017-0494-4.

[2] Безопасность в Интернете вещей: Международная конференция по компьютерным наукам и электронной инженерии «Безопасность Интернета вещей: текущие проблемы и возможности для исследований», Маккей К.А., Бассам Л., Туран М.С., Моуха Н. (2016), доклад о облегченной криптографии. ПРОЕКТ NISTIR, стр. 1-29

[3] С. Чандра, С. Пайра, С. С. Алам и Г. Саньял, «Сравнительный обзор криптографии с симметричным и асимметричным ключом», 2014 г., междунар. конф. Электрон. Коммуницировать. Вычислять. Анг. ICECCE 2014, стр. 83-93, 2014.

[4] Саурабх Сингх, Прадип Кумар Шарма, Со Ен Мун, Чон Хек Парк. Усовершенствованные облегченные алгоритмы шифрования для устройств Интернета вещей: обзор, проблемы и решения.

[5] К. А. Лара-Нино, А. Диас-Перес и М. Моралес-Сандовал, “Упрощенная криптография с эллиптическими кривыми: обзор”, IEEE Access, vol. PP, № c, стр. 1-1, 2018.

[6] Джеймс М., Кумар Д.С., Реализация модифицированного облегченного расширенного стандарта шифрования. Технология производства 25:582-589 (2016)

[7] Масрам Р., Шахаре В., Абрахам Дж., Муна Р., Синха П., Сандер Г., Попхалкар С. (2014a) Динамический выбор криптографических алгоритмов с симметричным ключом для защиты данных на основе различных параметров. Препринт arXiv arXiv: 1406.6221, стр. 1-8

[8] Масрам Р., Шахаре В., Абрахам Дж., Муна Р. (2014b) Анализ и сравнение криптографических алгоритмов с симметричным ключом, основанных на различных характеристиках файлов. В сети опубликовано приложение 6(4):43-52

[9] Маккей К.А., Бэшем Л., Туран М.С., Муха Н. (2016) Доклад о легковесной криптографии. ПРОЕКТ NISTIR, стр. 1-29.

REFERENCES*

[1] Oblegchennye algoritmy shifrovanija - https://link.springer.com/article/10.1007/s12652-017-0494-4.

[2] Bezopasnost' v Internete veshhej: Mezhdunarodnaja konferencija po komp'juternym naukam i jelektronnoj inzhenerii «Bezopasnost' Interneta veshhej: tekushhie problemy i vozmozhnosti dlja issledovanij», Makkej K.A., Bassam L., Turan M.S., Mouha N. (2016), doklad o oblegchennoj kriptografii. PROEKT NISTIR, str. 1-29

[3] S. Chandra, S. Pajra, S. S. Alam i G. San'jal, «Sravnitel'nyj obzor kriptografii s simmetrichnym i asimmetrichnym kljuchom», 2014 g., mezhdunar. konf. Jelektron. Kommunicirovat'. Vychisljat'. Ang. ICECCE 2014, str. 83-93, 2014.

[4] Saurabh Singh, Pradip Kumar Sharma, So En Mun, Chon Hek Park. Usovershenstvovannye oblegchennye algoritmy shifrovanija dlja ustrojstv Interneta veshhej: obzor, problemy i reshenija.

[5] K. A. Lara-Nino, A. Dias-Peres i M. Morales-Sandoval, "Uproshhennaja kriptografija s jellipticheskimi krivymi: obzor", IEEE Access, vol. PP, № c, str. 1-1, 2018.

[6] Dzhejms M., Kumar D.S., Realizacija modificirovannogo oblegchennogo rasshirennogo standarta shifrovanija. Tehnologija proizvodstva 25:582-589 (2016)

[7] Masram R., Shahare V., Abraham Dzh., Muna R., Sinha P., Sander G., Pophalkar S. (2014a) Dinamicheskij vybor kriptograficheskih algoritmov s simmetrichnym kljuchom dlja zashhity dannyh na osnove razlichnyh parametrov. Preprint arXiv arXiv: 1406.6221, str. 1-8

[8] Masram R., Shahare V., Abraham Dzh., Muna R. (2014b) Analiz i sravnenie kriptograficheskih algoritmov s simmetrichnym kljuchom, osnovannyh na razlichnyh harakteristikah fajlov. V seti opublikovano prilozhenie 6(4):43-52

[9] Makkej K.A., Bjeshem L., Turan M.S., Muha N. (2016) Doklad o legkovesnoj kriptografii. PROEKT NISTIR, str. 1-29.

Жексен Сейітбатталов, оқытушы, Л. Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан, sbtl.jeks@gmail.com

Шаттық Қанбаева, жетекші маман, «Мемлекеттік техникалық қызмет» АҚ, Астана, Қазақстан, shattyk.98.05@mail.ru

Махсут Бекенов, доцент, Л. Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан, bekenov50@mail.ru

Олжас Тасмагамбетов, докторант, Л. Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан, 5999452@mail.ru

Гульнара Тулешева, доцент, Satbayev University, Алматы, Казахстан, g.tulesheva@satbayev.university

ШЕКАРАЛЫҚ ЕСЕПТЕУЛЕР МЕН ЗАТТАР ИНТЕРНЕТІНІҢ (IOT) ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУГЕ АРНАЛҒАН ИНТЕЛЛЕКТУАЛДЫ ТӨМЕН РЕСУРСТЫ КРИПТОГРАФИЯЛЫҚ АЛГОРИТМДЕР

Аңдатпа. Мақалада Заттар Интернетінің (IoT) және шекаралық есептеу технологиясының заманауи дамуы, сонымен қатар ақпараттық қауіпсіздікті қамтамасыз ету жолдары мен IoT желілерінің әртүрлі деңгейлері арасындағы өзара әрекеттесу протоколдары қарастырылған. Қолданыстағы қауіпсіздік әдістері IoT құрылғыларының

есептеу және энергетикалық ресурстарына жоғары талаптар қояды. Осы мәселелерді шешу үшін IoT құрылғысы мен анық емес логикалық шекаралық түйіндердің келесі параметрлерін талдау қажет: деректер өлшемі, жады көлемі, желі сыйымдылығы, есептеу қуаты және батарея қуаты. Зерттеу нәтижесінде, осы параметрлерді талдау негізінде заттар Интернетінің шекаралық түйіндері арасындағы өзара әрекеттесудің оңтайлы алгоритмін таңдау, энергия тұтыну деңгейін оңтайландыру және есептеу ресурстарын пайдалану, және де қауіпсіздікті арттыру үшін интеллектуалды модель ұсынылды.

Түйінді сөздер. Заттар Интернеті (IoT), шекаралық түйіндер (шеткі түйіндер), жақсартылған гибридті жеңіл алгоритм (EHLA), төмен ресурсты криптография, протокол, шифрлау алгоритмдері, ақпараттық қауіпсіздік.

Zhexen Seitbattalov, teacher, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, sbtl.jeks@gmail.com

Shattyk Kanbayeva, leading specialist, «State Technical Service» JSC, Astana, Kazakhstan, shattyk.98.05@mail.ru

Makhsut Bekenov, docent, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, bekenov50@mail.ru

Olzhas Tasmagambetov, doctoral student, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, 5999452@mail.ru

Gulnara Tulesheva, docent, Satbayev University, Almaty, Kazakhstan, g.tulesheva@satbayev.university

INTELLIGENT LOW-RESOURCE CRYPTOGRAPHY ALGORITHMS TO SECURE BOUNDARY COMPUTING AND THE INTERNET OF THINGS (IOT

Abstract. The article presents the modern development of the Internet of things (IoT) and frontier computing technology, as well as considers ways to ensure the security of information and interaction protocols between different levels of IoT networks. The existing security methods make high demands on the computing and energy resources of IoT-devices. To solve all these problems, it is necessary to analyze the following parameters of IoT-device and fuzzy-logic boundary nodes: data size, memory volume, network capacity, computing power and battery power. As a result, on the basis of the analysis of these parameters, an intelligent model was proposed for selecting an optimal algorithm of interaction between boundary nodes of the Internet of things, optimizing the level of energy consumption and use of computing resources of the node, as well as improving safety.

Keywords. Internet of things (IoT), edge nodes, Enhanced hybrid lightweight algorithm (EHLA), low-resource cryptography, protocol, encryption algorithms, information security.

****