Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
Информатики и радиоэлектроники

УДК 004.77

Анисимова
Юлия Николаевна

Методика оценки параметров устройств интернета вещей при реализации ими симметричных криптографических алгоритмов

АВТОРЕФЕРАТ

на соискание степени магистра технических наук

по специальности 1-98 80 01 Информационная безопасность

_____

Научный руководитель
Власова Галина
Александровна
к.т.н, доцент

_____

Минск 2021

ВВЕДЕНИЕ

Развитие сетевых технологий в настоящее время приводит к ежегодному значительному увеличению количества устройств, способных обмениваться информацией между собой, а также получать ее от окружающей среды. Это привело к созданию концепции под названием «Internet of Things» – «Интернет вещей» (IoT), все более набирающей популярность в настоящий момент времени. Основой концепции служит сеть физических объектов, наделенных технологиями, позволяющими им взаимодействовать между собой, а также с внешней средой. Интернет вещей предполагает следующий подход к окружающей действительности: любой физический или рукотворный объект, которому может быть присвоен IP-адрес, и который может передавать данные в сети, является частью глобальной сети. В частности, такой «вещью» может являться человек с сердечным имплантатом, датчик давления в колесе современного автомобиля, и многие другие объекты.

Наиболее серьезной проблемой развития интернета вещей является проблема безопасности. Чем больше «умных» устройств подключается к сети, тем выше риски, связанные с несанкционированным доступом в IoT-систему и использованием ее возможностей злоумышленниками. Сегодня усилия многих компаний и организаций в сфере IT направлены на поиск решений, которые позволят минимизировать угрозы, тормозящие полноценное внедрение IoT. Развитие концепции Интернета вещей и ее внедрение в различные сферы предусматривает наличие десятков миллиардов автономных устройств. По данным портала Statista в 2017 году их уже насчитывается более 20 млрд, а к 2025 году ожидается не менее 75 млрд. Все они подключены к Сети и передают через нее соответствующие их функционалу данные. И данные, и функционал являются мишенью для злоумышленников, а значит, должны быть защищены.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Применение традиционных методов защиты устройств интернета вещей, таких как шифрование, идентификация/аутентификация и внедрение физических мер обеспечения безопасности, требует их существенного реинжиниринга и адаптации, так как устройства имеют множество ограничений. Интернет вещей, как правило, состоит из портативных устройств с низким электропотреблением, малым форм-фактором и ограниченными возможностями. В виду ограничений защитой от манипуляций и кибератак в

контексте IoT оптимальным вариантом являются микроконтроллеры, и основным средством обеспечения информационной безопасности в мире интернета вещей является так называемая «облегченная» криптография.

Связь работы с приоритетными направлениями научной, научно-технической и инновационной деятельности

Тема диссертационной работы соответствует разделу 6 «Обеспечение безопасности человека, общества и государства» приоритетных направлений научной, научно-технической и инновационной деятельности в Республики Беларусь на 2021–2025 гг., утверждённых Указом Президента Республики Беларусь 7 мая 2020 г., № 156. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цель и задачи исследования

Цель исследования – разработка методики оценки параметров устройств интернета вещей при реализации ими симметричных криптографических алгоритмов.

Предметом исследования являются устройства интернета вещей, при помощи которых реализуются криптоалгоритмы; симметричные криптографические алгоритмы, которые могут быть применены в микроконтроллерах малой производительности. Объектом исследования являются параметры легковесных симметричных криптоалгоритмов, характеристики устройств интернета вещей, при помощи которых реализуются легковесные симметричные криптоалгоритмы.

Задачи исследования – выбор и адаптация облегченного симметричного криптоалгоритма для использования на микроконтроллере, сравнение возможностей применения симметричных криптоалгоритмов на устройстве малой производительности с применением симметричных криптоалгоритмов в программной среде.

Апробация результатов диссертации

Основные положения и результаты диссертации опубликованы в сборнике XVII Международной научно-практической конференции «Управление информационными ресурсами» (Минск, 2021).

Опубликованность результатов исследования

По результатам исследований, представленных в диссертации, опубликовано 2 статьи в сборниках материалов конференций.

Теоретическая и практическая значимость

Теоретическая значимость работы заключается в разработанной методике оценки параметров микроконтроллеров, реализующих шифрование видео-данных симметричными криптоалгоритмами.

Практическая значимость заключается в реализации шифрования видео-данных в среде симуляции микроконтроллера симметричным легковесным криптоалгоритмом, где выбор устройства основан на теоретическом анализе характеристик существующих микроконтроллеров, выбор симметричного криптографического алгоритма основан на практических результатах их реализации программным методом.

Личный вклад соискателя

Работа полностью выполнена лично магистрантом на базе его исследований, реализованы программным методом симметричные криптографические алгоритмы, на основе полученных данных выбран алгоритм с лучшими показателями быстродействия и криптостойкости для его реализации аппаратно-программным методом; разработана оценка параметров устройств интернета вещей на основе полученных данных: зависимость процентного отношения быстродействия криптоалгоритма, реализованного разными методами (программным и аппаратно-программным), от полной стоимости системы видеосвязи (IP-камера и микроконтроллер).

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В первой главе представлен литературный обзор по теме исследования, введение в предметную область, описываются проблемы обеспечения безопасности таких устройств интернета вещей, как IP-камеры, представлен принцип обеспечения безопасности устройств интернета вещей, базовое знакомство с легковесной криптографией и требованиями

к реализации легковесных криптографических алгоритмов.

Во второй главе приводится классификация IP-камер, классификация симметричных криптоалгоритмов, классификация устройств интернет вещей, реализующих криптографические алгоритмы.

В третьей главе определены шаги методики оценки параметров устройств интернета вещей при реализации ими симметричных криптографических алгоритмов.

В четвертой главе по пунктам третьей главы определены оптимальные характеристики исследуемых криптоалгоритмов и микроконтроллеров для поставленной задачи обеспечения шифрования видеопотока, выбраны среды реализации криптографических алгоритмов программным и аппаратно-программным методами; реализованы программным методом симметричные криптографические алгоритмы, на основе полученных данных выбран алгоритм с лучшими показателями быстродействия и криптостойкости для его реализации аппаратно-программным методом, разработана оценка параметров устройств интернета вещей на основе полученных данных.

ЗАКЛЮЧЕНИЕ

Были исследованы легковесные криптоалгоритмы для шифрования ими видеопотока. Для этого в ходе исследования были программно реализованы восемь криптоалгоритмов – IDEA, CAST5, 3DES, BLOWFISH, SPECK, TWOFISH, CAMELLIA, AES. В сравнении криптоалгоритмов, реализующих шифрование видео-данных, учитывались такие характеристики алгоритмов, как длина информационного блока, длина ключа, число раундов (циклов шифрования), влияющие на криптостойкость алгоритма, и количество условных логических элементов. Оптимальным вариантом с точки зрения достаточной криптостойкости, которая была определена параметром размера ключа в не менее, чем 128 бит, и скорости шифрования, оказался алгоритм AES – алгоритм показывает наилучшее соотношение между временем шифрования и размером видеофайла. Были теоретически исследованы микроконтроллеры для определения оптимального микроконтроллера с наибольшей производительностью. Была выполнена симуляция микроконтроллера с обоснованием модели и симулятора. Исходя из полученных данных, можно утверждать, что аппаратно-программное шифрование уступает по показателям скорости программному шифрованию, однако аппаратно-программное шифрование обеспечивает достаточно высокую скорость шифрования и дешифрования получаемых данных, что

позволяет выполнять шифрование непрерывного потока информации.

Разработана оценка параметров устройств интернета вещей на основе полученных данных: зависимость процентного отношения быстродействия криптоалгоритма, реализованного разными методами (программным и аппаратно-программным), от полной стоимости системы видеосвязи (IP-камера и микроконтроллер) для разных длин ключей шифрования.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

[1] Анисимова, Ю. Н. Применение облегчённых криптоалгоритмов для интернета вещей / Ю. Н. Анисимова, А. А. Савченко, Г. А. Власова // Инфокоммуникации: сборник тезисов докладов 56-ой научной конференции аспирантов, магистрантов и студентов БГУИР, Минск, 18 – 20 мая 2020 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск: 2020 – С. 47–49.

[2] Анисимова, Ю. Н. Особенности применения малоресурсных криптоалгоритмов для шифрования видеопотока / Ю. Н. Анисимова, Г. А. Власова // Сборник тезисов и докладов XVII Международной научно-практической конференции «Управление информационными ресурсами», 12 марта 2021 г. / Академия управления при Президенте Республики Беларусь. – Минск: 2021.