УДК 004.056.2

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ПОДПИСЕЙ В МАЛОМОЩНЫХ IOT УСТРОЙСТВАХ

Любавина П.Ю. (Университет ИТМО)
Научный руководитель – д.т.н., доцент Беззатеев С.В.
(Университет ИТМО)

Аннотация. Обеспечение достоверности информации в маломощных устройствах, является одной из проблем «Интернета вещей». В докладе рассмотрен способ решения с помощью использования одноразовой и/или многоразовой подписей.

Введение. Согласно определению, данному Министерством Цифрового развития, «Интернет вещей» – глобальная инфраструктура для информационного общества, обеспечивающая возможность предоставления сложных услуг путем соединения друг с другом вещей на основе существующих и развивающихся функционально совместимых информационно-коммуникационных технологий.
«Интернет вещей» устраняет разрыв между цифровым и физическим миром, что означает, что взлом устройств может иметь опасные последствия в реальном мире. Взлом датчиков, контролирующих температуру на электростанции, может заставить операторов принять катастрофическое решение; контроль над автомобилем без водителя также может привести к катастрофе. Но проблем, связанных с информационной безопасностью, в области «Интернета вещей» достаточно много. В контексте данного исследования рассматривается проблема достоверности передаваемой информации, и применение технологий цифровых подписей для решения проблемы достоверности.

Основная часть. Устройства «Интернета вещей» разделены на несколько категорий: устройство переноса данных, устройство сбора данных, сенсорное устройство, исполнительное устройство, устройство общего назначения. Но все они разные и имеют ограниченные возможности в устройствах. Это происходит с большинством компьютеров, потому что они имеют ограничения по мощности, обработке и памяти. Как следствие, они не управляются так, как должны быть усовершенствованные шаблоны безопасности, поэтому они подвергаются большему риску быть атакованными или подверженными дефектам.
Поэтому мы предлагаем такой способ решения проблемы достоверности в устройствах «Интернета вещей»: в мощных будет использоваться технология блокчейн, в маломощных цифровые подписи (Лампорта и Меркле). Но существуют некоторые проблемы с внедрением и дальнейшим использованием подписей для обеспечения достоверности. Например, схема подписи Лампорта имеет большой размер и пары из открытого и закрытого ключей, а для подписи Меркле требуется большое количество ресурсов памяти.
Чтобы устранить эти проблемы мы решили найти так называемый «экстремум» маломощных устройств «Интернета вещей». Т. е. найти значение, которое показывает предел памяти устройства для использования подписи. Например, сколько устройство будет работать до того момента как дерево Меркле достигнет своего предела. И после оптимизировать его так, чтобы устройство работало с деревом равное количество времени, как и его батарейка. Это требуется для экономии времени и материальных ресурсов, чтобы при замене батарейки можно было сразу заменять и подпись. Что касается подписи Лампорта, то тут предлагается найти, опять же, «экстремум» и оптимальную цепочку блоков.

Выводы. Для достижения поставленных в исследовании задач необходимо составить имитационную модель системы, где в маломощных устройствах будут использоваться подписи Меркле и Лампорта, после чего провести оценку адекватности системы.

Заключительным этапом исследования будет являться оценка достоверности информации, передаваемой по сети.

Любавина П.Ю. (автор)	Подпись
Беззатеев С.В. (научный руководитель)	Подпись