ГИБРИДНЫЙ КРИПТОГРАФИЧЕСКИЙ АЛГОРИТМ ЗАЩИТЫ ДАННЫХ В СЕНСОРНОЙ СЕТИ

С.А. ПЛЕТНЁВ

В настоящее время одним из новых актуальных направлений в области информационных технологий является создание нового вида сетевых систем — сенсорных сетей. Сенсорная сеть — это распределенная сеть необслуживаемых миниатюрных электронных устройств (узлов сети), которые осуществляют сбор данных о параметрах внешней среды и передачу их на базовую станцию посредством ретрансляции от узла к узлу с помощью беспроводной связи. Одной из важнейших проблем данного подхода является обеспечение безопасности информации, циркулирующей в пределах сенсорных сетей с учетом ограниченных ресурсов.

Несмотря на важность передаваемой информации, обеспечение удовлетворительного уровня безопасности в сенсорных сетях никогда не было легкой задачей. Из-за того, что сенсорные сети не только подвергаются атакам злоумышленников, но также обладают многими ограничениями в ресурсах. Сенсорные узлы, исходя из архитектуры и условий применения, являются устройствами с ограниченными ресурсами. Они имеют ограниченные вычислительные, энергетические ресурсы и небольшой запас внешней памяти.

В качестве механизма информационной безопасности предлагается гибридный блочный алгоритм защиты данных, основанный на вычислении битовой последовательности OTP (one-time pad — одноразовый блокнот) в качестве одноразового секретного ключа и MAC(message authentication code — код аутентичности сообщения).

Значение MAC вычисляется с помощью криптографического блочного алгоритма SkipJack в режиме сцепления блоков шифротекста. Алгоритм вычисления MAC в режиме сцепления блоков шифротекста эффективен и быстр, и факт того что в его основе блочный шифр также минимизирует использование памяти, которая является ограниченным ресурсом в сенсорных сетях. При использовании гибридного алгоритма передаваемый пакет данных составляет 23 байта, как следствие, он не является ресурсоемким.

Данный алгоритм обеспечивает целостность, конфиденциальность и аутентичность данных и сенсора. Ключевая последовательность используется только один раз для каждого сеанса передачи данных. Криптостойкость алгоритма основана на криптостойкостях исходного мастер ключа и алгоритма при вычислении MAC.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

С.А. ПЛЕТНЁВ

Беспроводная сенсорная сеть представляет собой распределенную, самоорганизующуюся и устойчивую к отказу сеть большого числа малогабаритных (до нескольких десятков тысяч) автономных электронных узлов, способных обмениваться сообщениями и ретранслировать их по беспроводному каналу связи. Одной из важнейших проблем данной технологии является обеспечение безопасности информации.

Требования к защите информации в беспроводной сенсорной сети можно классифицировать следующим образом:

Аутентификация: Поскольку в WSN передается важная критическая информация. Получатель должен удостовериться в том, что принятая информация получена от авторизованного источника.

Целостность: Данные при передаче могут быть изменены нарушителем. Потеря или повреждение данных может также произойти из-за ненадежной коммуникационной среды. Целостность данных гарантирует, что информация не изменена при передаче.

Конфиденциальность данных: Конфиденциальность гарантирует, что содержание сообщения, которое передается, никогда не раскрывается несанкционированным объектам. Шифрование является стандартным подходом для обеспечения конфиденциальности.

Сенсорные узлы, исходя из архитектуры и условий применения, являются устройствами с ограниченными ресурсами. Они имеют ограниченные вычислительные, энергетические ресурсы и небольшой запас внешней памяти.

На данный момент существуют протоколы безопасности, которые соответствуют ограничениям WSN и обеспечивают защиту от некоторых типов угроз. Основным из них является протокол безопасности в сенсорных сетях SPINS. Протокол SPINS обеспечивает криптографическую защиту информации на прикладном уровне и состоит из протокола SNEP и μTESLA. Протокол SNEP обеспечивает конфиденциальность, целостность и аутентичность данных. Протокол μTESLA обеспечивает аутентификацию данных при широковещательной рассылке по сети.

Криптографической основой протокола SNEP является блочный шифр RC5, изобретенный Р. Ривестом в 1995 году. Данный шифр очень непритязателен с точки зрения вычислительной мощности и требуемого объема памяти и поэтому хорошо подходит для применения в сенсорных сетях.

ИСПОЛЬЗОВАНИЕ ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫХ ФУНКЦИЙ ДЛЯ ЗАЩИТЫ ЦИФРОВЫХ УСТРОЙСТВ, РЕАЛИЗУЕМЫХ НА ПЛИС

А.А. ПРОЩЕРЯКОВ, А.А. ИВАНЮК

Использование программируемых логических интегральных схем (ПЛИС) в качестве элементной базы цифрового устройства предполагает возможность внесения изменений в синтезируемый проект как на этапе описания его на HDL-языках, так и уже в реализованный проект. Данный аспект позволяет злоумышленникам внести собственные вредоносные элементы в созданный проект, внедрять так называемые аппаратные трояны (Hardware Trojans), которые могут исказить функционирование цифрового устройства либо получить доступ на аппаратном уровне к конфиденциальной информации. В связи с этим актуальной является задача проектирования цифровых устройств, которые в автономном режиме проверяли бы целостность не только обрабатываемых данных, но и своей аппаратной составляющей. Данная методика проектирования получила название Design For Trust (DFT).

В качестве одного из походов к решению задач DFT предлагается применение физически неклонируемых функций (PUF, Physical Unclonable Function), которые основаны на использовании непредсказуемых и невоспроизводимых отклонений в физической структуре интегральных схем при их изготовлении. Внедрение специализированных типов PUF позволит решить следующие задачи: идентификация цифровых устройств, идентификация ПЛИС, аутентификация