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.