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

цифровых устройств при их реализации на ПЛИС, защита цифровых устройств от клонирования на идентичных ПЛИС, защита цифровых устройств от несанкционированных изменений.

ШИФРОВАНИЕ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ СИСТЕМ ФАЗОВОЙ СИНХРОНИЗАЦИИ

Д.Л. ШИЛИН, С.С. БЫВШЕВ, М.В. ПОЧЕБУТ

Авторами предлагается способ шифрования данных с использованием систем фазовой синхронизации (СФС), работающих в режиме детерминированного хаоса. Данный режим работы является нерегулярным. Причина нерегулярности определяется свойством нелинейных систем экспоненциально быстро разводить первоначально близкие траектории. Поэтому не представляется возможным предсказать поведение таких систем, так как реально начальные условия можно задавать лишь с конечной точностью, а ошибки экспоненциально возрастают.

Предлагается на основе ранее разработанной имитационной модели СФС создать систему шифрования информации для передачи последней по открытым каналам связи. В качестве случайных последовательностей будут использоваться значения фазы и частоты сигнала на выходе блока фильтров модели. Будет использован симметричный алгоритм шифрования, в котором шифрование и дешифрование отличается только порядком выполнения и направлением некоторых шагов. В этом алгоритме авторами предлагается использовать один и тот же секретный ключ — физические параметры работы модели. С точки зрения простоты реализации, наиболее привлекательным является двоичное (битовое) гаммирование. Обычно, при использовании гаммирования, если гамма короче, чем открытое сообщение, она повторяется требуемое число раз. В нашем случае, в этом нет необходимости, так как возможно сгенерировать гамма последовательность необходимой длины. Этот аспект позволяет построить поточную систему шифрования данных, которая сможет передавать поток данных, каждый символ которых должен быть зашифрован и отправлен куда-либо, не дожидаясь последующих данных (обмен текстовыми и голосовыми сообщениями по сети).

При кодировании файла целиком (без учета структуры), снижается криптостойкость шифра. Это объясняется тем, что многие файлы помимо основных данных, хранят однородные данные о формате. Поэтому для некоторых форматов файлов целесообразно шифровать только основные данные.

СИСТЕМА КОНТРОЛЯ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ БУРОВОЙ УСТАНОВКИ

М.В. ПОЧЕБУТ, Ю.В. ВОРОБЬЕВА

Для обеспечения операций бурения используются дизельные двигатели большой мощности. Ежедневно мастер готовит отчет о работе технологического оборудования на буровой установке и по телефону докладывает информацию в диспетчерскую службу бурового предприятия. Такой контроль сложно назвать надежным, так как присутствует человеческий фактор, влияющий на достоверность передаваемой информации.

Целью данного проекта является проектирование системы по обеспечению оперативного мониторинга и контроль в режиме ON-LINE работы, к примеру, всех