Эссе по курсу "Защита информации", кафедра радиотехники,
Московский физико-технический институт (ГУ МФТИ),
http://www.re.mipt.ru/infsec

Безопасность в беспроводных сенсорных сетях

Фимин Александр

19 апреля 2007 года

г. Долгопрудный

Непрекращающийся научный прогресс в микроэлектронике и компьютерной технике ведет к усовершенствованию современных технологий производства электронных компонентов. Экспоненциально сокращаются как размеры, так и стоимость полупроводниковых устройств, улучшаются их энергетические характеристики [1]. Всё это позволяет исследователям проектировать и использовать миниатюрные устройства для широкого класса задач. Беспроводные сети находят применение в задачах контроля состояния среды, там, где данные необходимо получать от большого количества узлов, или там, где развертывание обширной проводной сети невозможно по каким-либо причинам.

Беспроводная сенсорная сеть - это множество автономных устройств, собирающих и обрабатывающих информацию об окружающем мире, и способных обмениваться этой информацией, используя каналы радиосвязи. Каждый элемент такой сети помимо одного или нескольких датчиков, как правило, содержит источник питания (батарею), микроконтроллер, и маломощный радиоприемник/передатчик. Стоимость такого небольшого изделия обычно невысока, что позволяет использовать до нескольких сотен, а возможно и тысяч таких устройств, образующих единую сеть. Однако чтобы использовать собранную информацию необходимо обеспечить передачу данных со всех устройств сети на один или несколько так называемых базовых узлов. Базовые узлы обладают стабильным источником питания, большими вычислительными мощностями и сопряжены с проводной сетью. Радиоканалы отличаются особенной степенью уязвимости, поэтому во многих гражданских и особенно военных применениях необходимо обеспечивать безопасность передачи данных.

Конкретно, можно проследить, какую специфику приобретают следующие криптографические задачи для сенсорных сетей:

Конфиденциальность данных

Так как существует возможность «прослушать» связи необходимо скрыть информацию. Один из способов это сделать – шифрование ключом, который известен только легальным получателям. Возможны схемы с использованием закрытых и открытых ключей.

Аутентификация данных

На этапе построения сети очень важно быть уверенным, что сообщения приходят от корректного источника. В случае удачных атак могут произойти критические изменения (например, перепрограммирование сети, изменение циклов синхронизации), что способно привести не только к утечке данных, но и к полному прекращению функционирования. Например, противник может сразу же передавать в эфир информацию, полученную от одного сенсора другому сенсору в любом месте сети с какой либо задержкой. При стандартном обмене информации получатель и приемник могут хранить один ключ, зашифровав сообщения которым, они могут идентифицировать друг друга. При широковещательной рассылке такой механизм не подходит, так как каждый получатель знает ключ и, следовательно, может имитировать поведение отправителя.
Поэтому при широковещательном способе передачи желательно использовать асимметричные алгоритмы[1,3,6].

Целостность данных

Целостность данных можно рассматривать как проблему подтверждения того, что данные, принятые приемником это те самые данные, которые послал источник, они не были изменены по пути. Эта задача может быть даже важнее, чем конфиденциальность данных, например, в приложениях обнаружения вторжения или пожарных системах.

Свежесть данных

Необходимо обеспечивать свежесть данных, то есть определять время отправки пакета, с тем, чтобы отбрасывать устаревшие сообщения и не позволять возможным злоумышленникам повторно передавать перехваченные сообщения.

Атаки на сенсорные сети

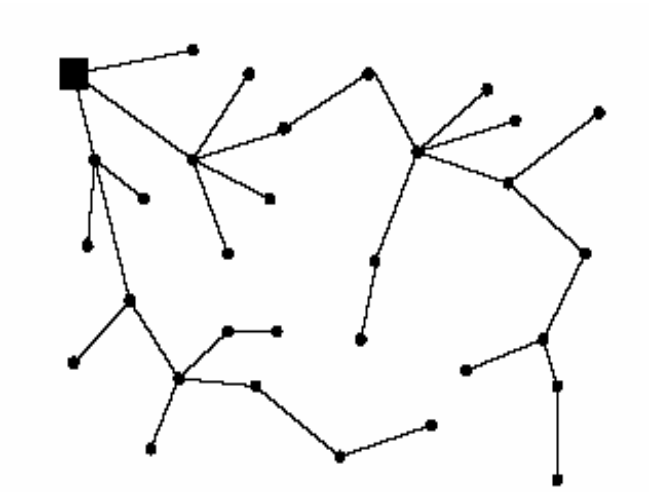
Из-за неопределенной заранее структуры сети, необходимости передавать маршрутную информацию, а также легкости доступа к каналам возникает целый ряд специфичных для беспроводных сенсорных сетей угроз.
Атаки могут производиться на всех уровнях модели OSI. Вот несколько примеров

Ложная маршрутная информация

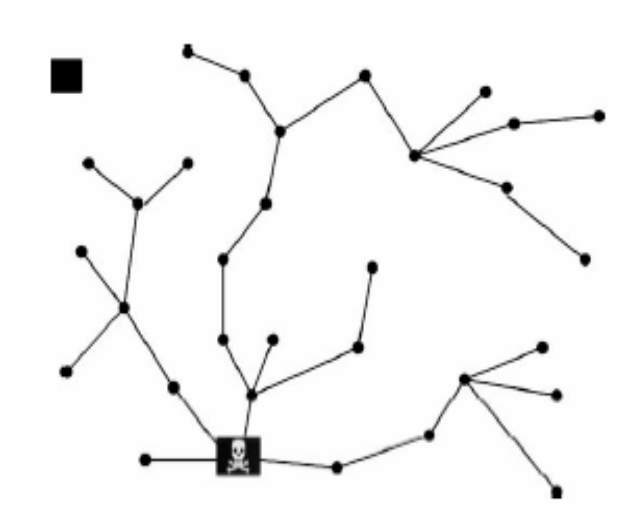
Этот тип атак ориентирован на маршрутные сообщения, которыми обмениваются сенсорные узлы. Сначала злоумышленник получает доступ к среде, имитируя поведение сенсорного узла. Поступающие ему маршрутные сообщения он изменяет и распространяет по определенной схеме.

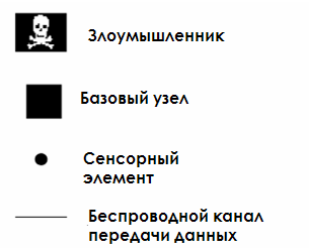
Последствиями такой атаки могут стать образование циклов передачи информации, притягивание или отталкивание трафика к месту вторжения, увеличение или уменьшение маршрутных путей, дробление сети, увеличение задержки и т.п. Этот вид позволяет злоумышленнику выборочно скрывать информацию.

Пример сетевой структуры до атаки



Вид сети после атаки.



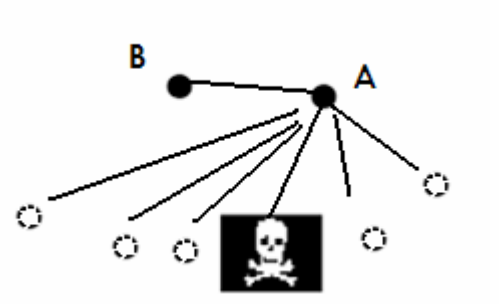


Выборочная пересылка

Цель данного вида атаки – остановить распространение некоторых сообщений с помощью внедренных в сеть узлов. Если узел злоумышленника находится на пути распространения сообщения, оно не пересылается. Если злоумышленник способен определить момент передачи, он может просто создать коллизию в нужный момент. Для того, чтобы как можно больше путей проходило через компрометированный узел, он делается наиболее привлекательным для своего окружения (сильный сигнал, небольшое количество пересылок до базового узла).

Атака с созданием множества виртуальных узлов

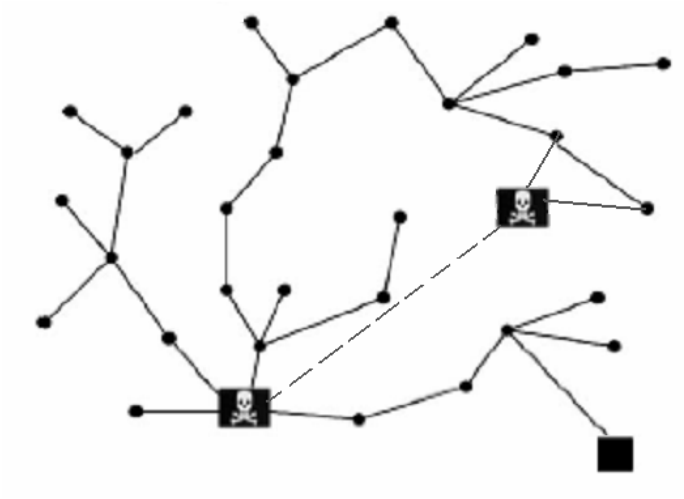
Из-за того, что любой сенсорный узел не знает всей топологии сети, один и тот же узел злоумышленника может выступать в роли нескольких узлов. Это может привести к уменьшению эффективности схем, основанных на использовании нескольких путей, нарушить целостность данных и т.п.



Туннельные атаки

Перехваченные сообщения в таком типе атак по высокоскоростным каналам распространяются в разные места сети, после чего воспроизводятся. В результате может образоваться нежелательный канал между удаленными друг от друга узлами.

Эта чрезвычайно эффективная атака позволяет злоумышленнику с минимальным знанием об алгоритмах используемых при передаче данных прослушивать, и воздействовать на большое количество трафика.



Пример защищенного протокола SNEP

В качестве примера протокола использующего криптографическую защиту данных рассмотрим протокол SNEP[5,6].

Криптографической основой подсистемы безопасности является блочный шифр RC5, изобретенный Р. Райвестом 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. Шифрование производится над блоком данных, состоящим из двух слов, обозначаемых *A* и *B*. На каждом из *r* раундов производятся следующие операции:

$$A = ((A \oplus B) <<< B) + S_{2i}$$

$$B = ((B \oplus A) <<< A) + S_{2i+1}$$

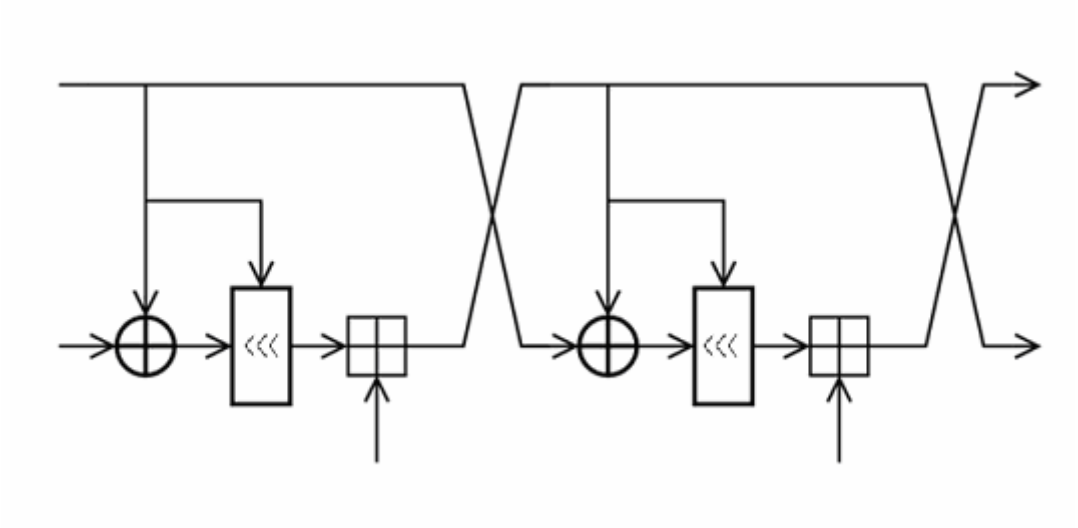
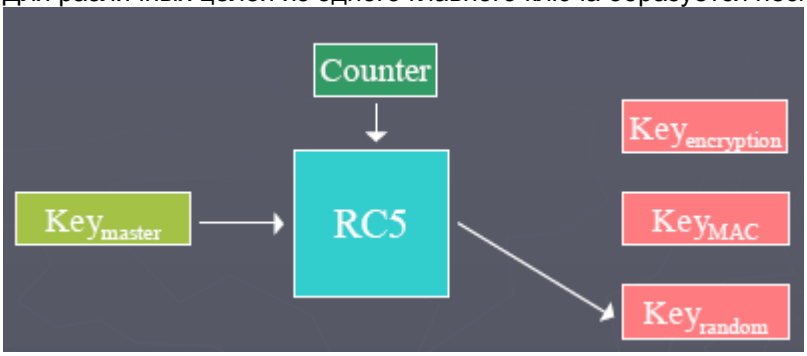


Схема двух “полураундов” RC5

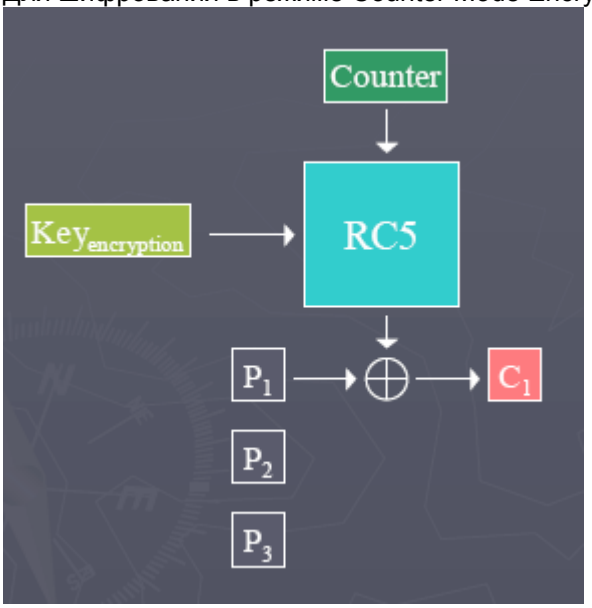
Здесь *S* – массив из 2*r*+2 слов, получающихся в результате процедуры развертки ключа. Символом "⊕" обозначается операция XOR, а "<<<" – циклический сдвиг влево.

Для базового узла и узла собирающего информацию общим является предустановленный главный ключ.

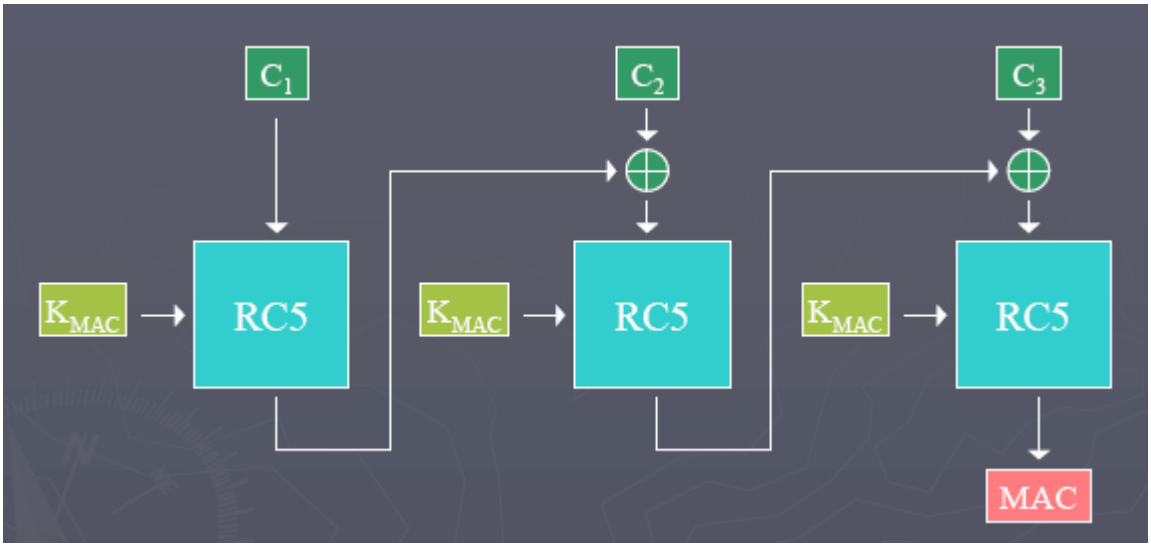
Для различных целей из одного главного ключа образуется несколько.

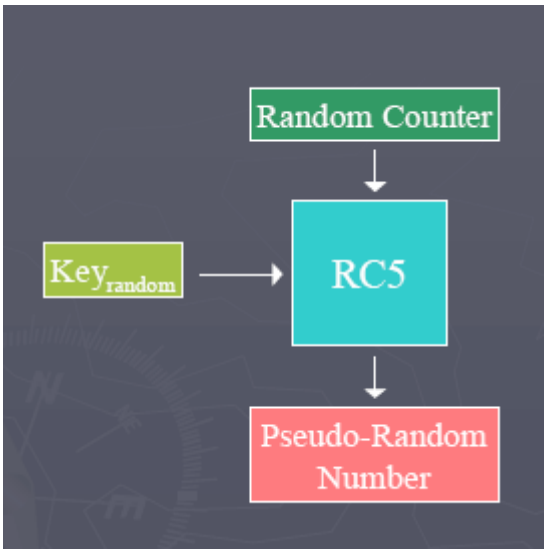


Для шифрования в режиме Counter Mode Encryption



Для целей аутентификации сообщения в режиме Cypher Block Chaining

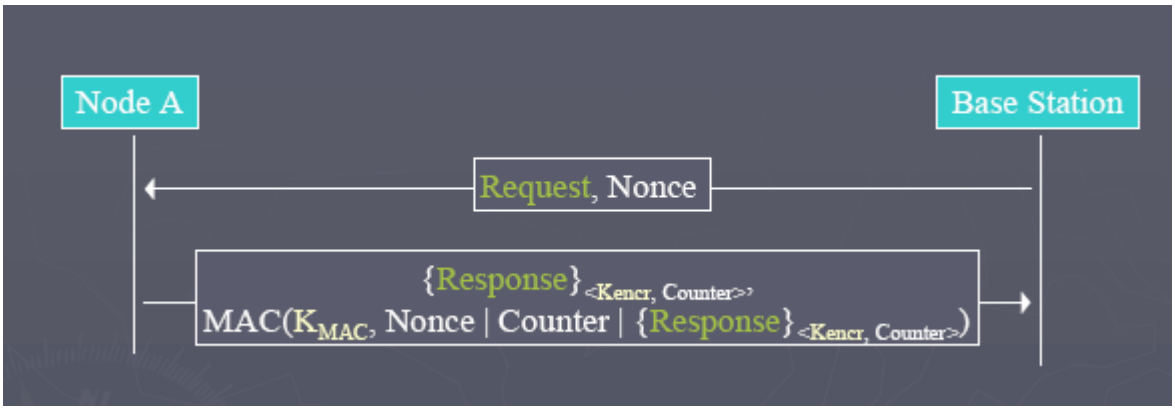




Для обеспечения “свежести” данных, вычисления параметра Nonce.

Если счетчик переполняется, новый ключ получается из последнего ключа и главного ключа.
$K_{random}' = MAC(K_{master}, K_{random})$

Схема, в случае необходимости обеспечения “сильной свежести” данных выглядит так: Базовый узел генерирует параметр Nonce случайным образом и включает его в запрос. Сенсорный узел шифрует сообщение обычным способом, но в MAC добавляет Nonce.



Недостатком протокола служит большое количество ключей, которые необходимо хранить для каждой пары приемник – передатчик, поддержание синхронизированных счетчиков, обязательность предварительной установки ключей.

Все это делает протокол SNEP неприменимым в приложениях с большим количеством межузловых одноранговых связей.

Существуют мнения [1,4], что асимметричные криптографические алгоритмы, такие, как, например, RSA, не пригодны для обеспечения безопасности в сенсорных сетях из-за ограниченных вычислительных, энергетических ресурсов, а также ресурсов памяти небольших сенсорных устройств и ограниченной пропускной способности радиоканалов.

Тем не менее, последние исследования показали реальность использования асимметричных схем, таких как, например, алгоритм ECC базирующийся на криптографии с использованием эллиптических кривых [3].

Список литературы

[1] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar “SPINS: Security Protocols for Sensor Networks (2002 ,Wireless Networks Journal)
[3] Mitch Blaser “Enabling security in industrial wireless sensor networks”
(May 9 2006,Industrial Embedded Systems, http://www.industrial-embedded.com/articles/blaser/)
[4] А.Д.Фомин, А.В.Фомина “Организация системы безопасности в сенсорных сетях”
(2004, http://nit.miem.edu.ru/2004/section/237.htm)
[5] Rishi Pidva “Security in Wireless Sensor Networks” (March 3 2003,
http://www.cs.wmich.edu/wsn/doc/spins/Pidva_SPINS.pdf)
[6] Mengke Li “Secure Routing Protocols in Wireless Sensor Networks“ (November 2004,
http://cse.unl.edu/~hcheng/courses/csce990/mli-cse990F2004.ppt)