РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ ДЛЯ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОЙ ПЕРЕДАЧИ ДАННЫХ В СЕНСОРНЫХ СЕТЯХ

В.В. Акудович, Г.Ф. Астапенко
Беларусь, г. Минск

ВВЕДЕНИЕ

Во многих специализированных приложениях возникает необходимость сетевой передачи конфиденциальной информации, при этом одной их основных проблем является обеспечение надежности используемых криптографических протоколов. Уязвимость протоколов в первую очередь связана с потенциальной возможностью компрометации клиентов связи, обладающих ключевой информацией. В том случае, когда секрет (ключи) разделяется между несколькими клиентами в группе (с использованием так называемых пороговых схем), устойчивость (по отношению к криптоатакам) используемых протоколов передачи конфиденциальных данных существенно повышается. При использовании подобных протоколов в сетях с ограниченными ресурсами (например, в сенсорных) возникают следующие проблемы:

- координация узлов и децентрализованное распределение ключевой информации;
- оперативная коррекция протокола взаимодействия в случае компрометации узла (канала) сети;
- реализация достаточно сложных в вычислительном плане алгоритмов с приемлемым быстродействием.

Узлы сенсорной сети не могут использовать асимметричную криптографию напрямую, поскольку обладают ограниченной вычислительной мощностью и ограниченной памятью. Поэтому сам узел не может постоянно генерировать асимметричные схемы и создавать большую базу открытых ключей. Поэтому существующие на данный момент криптографические протоколы для сенсорных сетей базируются на симметричной криптографии.

Основной способ создания общего шифрованного канала между двумя узлами или узлом и базой (выделенным узлом, выполняющим функции диспетчера сети) – это создание между ними сеансового ключа. Из-за вычислительной и энергетической ограниченности узлов, подход, аналогичный в обычных сетях, не применим.

Стандартный подход в сенсорных сетях для решения этой проблемы - это внедрение в каждый узел некоторой информации, сгенерированной базой. Причем информация внедряется до установления конфигурации сенсорной сети. На базе данной информации два узла, или база и узел, пытаются провести взаимную аутентификацию и установить сеансовый ключ для шифрования данных.

Существует несколько видов распределения ключей в сенсорных сетях: схема Eschenauer и Gligor случайного распределения ключа [1], схема q-композиции случайного ключа [2], схема многомерного ключевого распределения [2], схема полиномиального распределения ключа [3].

В данной работе предлагается метод образования ключей на базе пороговой схемы. Данный метод не использует средств ассиметричной криптографии. Вычислительные затраты, которые предлагается выполнять узлам, меньше вычислительных затрат, необходимых на создание пороговой схемы. В работе предложена схема образования ключей с использованием разделения секрета в сенсорных сетях, которая позволяет при этом максимально уменьшить вычислительные затраты.

1. СХЕМА РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ НА БАЗЕ ПОРОГОВОЙ СХЕМЫ ШАМИРА

Для формирования сеансового ключа, используемого узлами сенсорной сети, необходимо наличие некоторой информации, которая позволяет создать данный ключ. Эта информация внедряется в узлы сети еще до установления конфигурации сети. Поэтому во время образования сеансовых ключей доверие основывается на той информации, которую в узел внедрила база. Поэтому схема распределения ключей играет самую главную роль в криптографии для сенсорных сетей, поскольку от нее зависит эффективность работы всей сети в дальнейшем.

Далее рассмотрим схему распределения ключей на базе пороговой схемы Шамира. При разработке данной схемы была учтена специфика сенсорной сети: по возможности основная часть вычислительной мощности переложена с узла на базу.

1. База генерирует множество ключей Ti, где i=1..n. Необходимо, чтобы число ключей n было больше, чем число узлов в сети N. В дальнейшем эти ключи будут использоваться для шифрования данных между двумя узлами симметричным алгоритмом. Затем каждый ключ разделяется по (t+1,m) пороговой схеме: Ti -> Sij, где i=1..n, j=1..m. Наиболее подходящей схемой является схема Шамира [4,5].

2. Каждый сенсор Nα получает от базы:

a) K0, Kα – индивидуальный ключ для общения с базой, Ma – индивидуальный ключ для подписи своих сообщений кодами аутентификации (MAC).

b) {Sij} – множество теней, где из каждой схемы каждому узлу выдается тень, причем эту тень ни один из других узлов не получит. То есть каждый узел получает уникальный набор теней. Причем мощность множества $|Sij| < n$, где n - количество всех схем, сгенерированных базой.

c) Ch(Sγi) – информация о доказательстве наличия тени из пороговой схемы Tγ другому узлу, при этом не раскрывая самой тени.

d) Par(Tγ) – параметры пороговой схемы: pγ-простое число, используемое в пороговой схеме Tγ; Hγ(z)-проверочная функция; xi – параметр, используемый в процессе получения тени Sγi из Tγ. Следует отметить, что Hγ(xi) = Ch(Sγi) – условие, используемое для доказательства наличия тени [6, 7].

e) Каждому узлу выдается набор симметричных ключей {Kt$_i$}, где каждый ключ соответствует конкретной пороговой схеме Ti. Количество ключей Kt$_i$, полученных узлом, равняется количеству пороговых схем, которыми данный узел обладает. Этот набор ключей в дальнейшем позволит узлам обмениваться тенями, для воссоздания секретного ключа.

Отличие пороговой схемы в предлагаемом протоколе от обычных пороговых схем – то, что максимально снижена нагрузка на узлы сети. Как известно, процесс генерации больших простых чисел pγ (в данной схеме они используются в пороговых схемах), достаточно сложен с вычислительной точки зрения. Поэтому генерацию простых чисел выполняет база, которая также выполняет и процесс разделения теней, а узлы получают уже готовую для работы информацию. Также база вычисляет и другие параметры пороговых схем: Ch(Sγi), Hγ(z).

2. ГЕНЕРАЦИЯ СЕАНСОВЫХ КЛЮЧЕЙ МЕЖДУ УЗЛАМИ

На основе полученной информации узлы должны установить между собой связи. Здесь возникает множество вариантов для образования ключа. Ниже рассмотрены некоторые основные случаи.

2.1. ОБРАЗОВАНИЕ КЛЮЧА МЕЖДУ УЗЛАМИ С ОБЩЕЙ ПОРОГОВОЙ СХЕМОЙ

Рассмотрим сенсорную сеть после установления (разброса датчиков). Пусть рядом находятся два узла Na и Nb, которые обладают общими пороговыми схемами. Протокол установления общего ключа:

1. Na->Nb: $E_{K0}(p_1)$, pi €A

2. Nb: pi €A, A∩B-> pγ€ A∩B
3. Nb->Na: $E_{K0}(Ch(S\gamma b),x_{\gamma b})$
4. Na: $H\gamma(x_{\gamma b})$= Ch(Sγb)
5. Na->Nb: $E_{K0}(Ch(S\gamma a),x_{\gamma a})$
6. Nb: $H\gamma(x_{\gamma a})$= Ch(Sγa)
7. Nb->Na: $E(Kt_\gamma, S\gamma b)$
8. Na->Nb: $E(Kt_\gamma, S\gamma a)$
9. Na,Nb: Tγ – если порог равен 2.

Вначале Na и Nb находят общую пороговую схему. Узел Nb выбирает схему, по которой будет восстановлен общий ключ. На шаге 3 Nb отсылает информацию о своей тени из схемы Tγ. Далее Na проверяет, что Nb обладает данной информацией. Аналогично на шагах 5,6 только Na доказывает наличие тени Nb. После этого узлы обмениваются зашифрованными тенями и, если порог равен двум, то они восстанавливают ключ. Следует отметить, что можно создать порог равным 3 и более, тогда, чтобы восстановить ключ, надо расширить этот протокол на большое количество участников. Ключи $\{Ks_i\}$ после установления контакта могут быть отброшены.

2.2. УСТАНОВЛЕНИЕ ОБЩЕГО КЛЮЧА МЕЖДУ ДВУМЯ УЗЛАМИ БЕЗ НАЛИЧИЯ ОБЩИХ ПОРОГОВЫХ СХЕМ

Возникновение данной проблемы зависит от общего числа пороговых схем, сгенерированных базой, а также от числа теней, которые получает каждый сенсор. Наличие этой проблемы сильно зависит от архитектуры сети. Если ближайшие сенсоры не обладают общими пороговыми схемами, то для установления общего ключа возможны несколько вариантов: создание ключа при помощи ближайших соседей или базы. Один из вариантов установления ключа при помощи базы рассмотрен в [8,9].

Основная идея выработки ключа между сенсорами без общей пороговой схемы – это поиск и заимствование теней у своих соседей, с которыми ранее уже был установлен контакт. Вероятность того, что у трех и более узлов найдется общая пороговая схема, значительно выше вероятности нахождения общей пороговой схемы у двух узлов.

После потери некоторых теней, соседние узлы при необходимости могут впоследствии запросить базу восполнить потерю. Однако, очевидно, что этим узлам придется доказать, что они действительно отдали свою тень соседу для установления ключа.

3. АНАЛИЗ РАЗРАБОТАННОЙ СХЕМЫ РАСПРЕДЕЛЕНИЯ СЕКРЕТА В СЕНСОРНОЙ СЕТИ

В данном разделе отметим некоторые особенности реализации и преимущества использования пороговых схем в сенсорных сетях.

На первоначальном этапе конфигурации сенсорной сети база генерирует схемы разделения с порогом более двух. Для восстановления ключа понадобится более двух узлов. При этом создается группа узлов, которая обладает общим ключом для своего канала. Понятно, что количество членов в группе может быть больше порога схемы. При этом некоторые участники группы (желательно все) образуют общие ключи с другими группами.

При компрометации одного из узлов, группа отсоединяется от скомпрометированного узла. При этом желательно, чтобы скомпрометированный сенсор не смог входить в контакт с нормальными сенсорами. Для этого необходимо раскрыть для всей сети тени, которыми обладает этот узел. Когда этот узел попытается вступить в контакт, другие узлы запросят идентификацию его теней, и легко смогут проверить, что он скомпрометирован.

Использование пороговых схем позволяет увеличить криптостойкость всей системы в целом. Особенно это заметно на примере компрометации одного узла, поскольку противник ничего не может узнать о поле ключей, используемом для связи между узлами. Максимально доступная для него информация – это ключи, которые восстановлены на узле в данный момент для связи с другими узлами и локальными группами. Поэтому для компрометации работы сети необходим более тонкий метод криптоатаки.

ЗАКЛЮЧЕНИЕ

В данной работе предложена новая схема распределения ключей на основе разделения секрета для конфиденциальной передачи данных в беспроводных сенсорных сетях. Данная схема позволяет обеспечить криптостойкость и функционирование в режиме конфиденциальной связи в случаях компрометации некоторого узла или канала связи.

Предложенная схема первоначального распределения ключей разработана таким образом, чтобы максимально снизить вычислительные нагрузки на узлы.

Литература

1. Laurent Eschenauer. Virgil Gligor. Key management scheme for distributed sensor network. Department of computer science University of Maryland, - 2002.

2. Lanlan Zhang. Secure communication in sensor network., - 2003.

3. Donggang Liu, Peng Ning.Establishing pairwise keys in distributed sensor network.. North Carolina State University, - 2002.

4. Брюс Шнайер. Прикладная криптография 2-е издание. Протоколы, алгоритмы и исходные тексты на языке С, - 1994.

5. Alfred J. Menezes, Paul C. Van Oorschot and Scott A. Vanstone. The Handbook of Applied Cryptography.-CPC press, - 1996.

6. Stanislaw Jarecki. Efficient threshold cryptosystem. Massachusetts institute of technology, - 1996.

7. Sughata Doshi. Dynamic secret redistributation. Information Networking Institute, - 2004.

8. Yei Wei Law, Ricardo Corin. Formally verified Decentralized key management architecture for wireless sensor network. Faculty of electric engineering of California, - 2003.

9. Adrian Perig, Victor Shewczyk. SPINS- Security protocol for sensor network. Department of computer science University of California, - 2001.