О ПРОБЛЕМЕ БЕЗОПАСНОСТИ СВЯЗИ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

Деундяк В.М.[1] , Таран А.А.[2]

Цель работы: *организация безопасной передачи данных в беспроводных сенсорных сетях при наличии внешних и внутренних злоумышленников.*

Методы исследования: *сравнительный анализ типов протоколов распределения ключей, исследование имеющихся подходов к построению схем организации защищенной связи в беспроводных сенсорных сетях, оценка энтропии предварительной ключевой информации.*

Результаты: *для беспроводных сенсорных сетей предлагается использование схем предварительного распределения ключей; строится модель такой схемы, обеспечивающая защиту от внешнего злоумышленника; исследуются требования на объем предварительной ключевой информации для каждого устройства в сети, исходя из требований на общий секретный ключ и устойчивость схемы к коалиционным атакам внутреннего злоумышленника; для борьбы с коалиционными атаками внутреннего злоумышленника предлагается использовать пороговые схемы предварительного распределения ключей, в частности, полилинейные и комбинаторные схемы, для которых рассматриваются вероятности успешного проведения атак в случае превышения злоумышленником порога; правильность полученных выводов подтверждается проведенными ранее исследованиями авторов.*

Ключевые слова: *беспроводные сенсорные сети, организация общих ключей, схемы предварительного распределения ключей, пороговые схемы, полилинейные схемы, комбинаторные схемы, коалиционные атаки.*

DOI: 10.21681/2311-3456-2020-03-13-21

Введение

Рассмотрим задачу обеспечения безопасной коммуникации между устройствами в беспроводных сенсорных сетях. Под сенсором понимается устройство, состоящее из системы мониторинга, предназначенной для сбора данных об окружающей среде, системы обработки данных, а также коммуникационной системы, предназначенной для передачи собранных данных [1, с. 103]. С помощью коммуникационной системы сенсоры могут обмениваться собранными данными с соседними сенсорами, тем самым образуя беспроводную сенсорную сеть. При этом общение напрямую между двумя произвольными узлами сети может быть не всегда возможно в силу потенциальной удаленности сенсоров друг от друга или наличия препятствий между ними. В этом случае данные могут передаваться через один или несколько промежуточных узлов. Для организации такой связи могут использоваться различные протоколы маршрутизации [1, с. 108], [2,3]. Однако, в конечном итоге любая передача данных между устройствами в сети сводится к серии последовательных передач между двумя соседними узлами сети, поэтому в данной работе ограничимся рассмотрением непосредственной передачи данных между двумя устройствами напрямую, без участия промежуточных узлов.

Отметим, что передача данных в сети осуществляется посредством беспроводных каналов связи, в которых эти данные могут быть легко перехвачены внешним наблюдателем. Из-за этого возникает задача обеспечения безопасности передачи данных между узлами, которая может решаться с помощью криптосистем, для работы которых требуется наличие у сторон общения общего секретного ключа. Таким образом, необходима разработка протоколов организации общих секретных ключей, учитывающих особенности беспроводных сенсорных сетей: ограничения на объем памяти и на ёмкость источника питания, необходимость автономной работы, возможность воздействия злоумышленника.

Целью работы является организация безопасной передачи данных в беспроводных сенсорных сетях. Для достижения этой цели используется сравнительный анализ типов протоколов распределения ключей, а также исследование имеющихся подходов к построению схем организации защищенной связи в беспроводных сенсорных сетях. Одни из таких схем требуют наличия у каждого устройства в сети большого объема памяти для хранения ключей. Другие схемы могут требовать меньший объем памяти, но при этом в них возникает возможность внутренних коалиционных атак, при которых внутренний злоумышленник, который смог получить ключевую информацию с нескольких устройств в сети, может получить доступ к данным, передаваемым между другими устройствами. Некоторые из таких схем гарантируют, что в случае, если размер коалиции, состоящей из устройств, ключевая информация с которых

1 Деундяк Владимир Михайлович, кандидат физико-математических наук, доцент, Южный Федеральный Университет, ФГНУ НИИ «Спецвузавтоматика», г. Ростов-на-Дону, Россия. ORCID: orcid.org/0000-0001-8258-2419. E-mail: vl.deundyak@gmail.com

2 Таран Алексей Александрович, аспирант, Южный Федеральный Университет, г. Ростов-на-Дону, Россия. ORCID: orcid.org/0000-0002-1357-9360. E-mail: fraktal-at@yandex.ru

была получена внутренним злоумышленником, не превышает некоторого порогового значения, то проведение коалиционной атаки будет невозможно. В случае превышения этого значения безопасность всех ключей в системе больше не гарантируется.

Поэтому представляется актуальным поиск наиболее подходящих схем с достаточно большими пороговыми значениями, требующих меньший объем памяти и обеспечивающих более безопасную передачу данных даже в случае превышения внутренним злоумышленником порогового значения.

В разделе 1 рассматриваются основные подходы к организации защищенной связи в беспроводных сенсорных сетях. На основе анализа этих подходов наиболее подходящей для таких сетей выбрана схема предварительного распределения ключей, и в разделе 2 на основе этого строится модель защищенной связи при наличии внешнего злоумышленника. Однако в построенной модели возникает угроза внутреннего злоумышленника, и в разделе 3 предлагается использовать пороговые схемы, предоставляющие защиту не только от внешнего злоумышленника, но и от коалиций внутреннего злоумышленника, мощность которой не превышает заданный порог, и рассматриваются примеры таких схем.

1. Подходы к решению задачи организации защищенной связи в беспроводной сенсорной сети

Для того, чтобы обеспечить безопасность передачи данных между сенсорами от внешнего злоумышленника, который может перехватывать передаваемые в сети сообщения, они должны иметь общий секретный ключ. Для организации секретных ключей используются протоколы распределения ключей. Различают следующие основные типы протоколов (см. [4, с. 55], [5]):

1) схемы предварительного распределения ключей, суть которых состоит в том, что предварительно распределяются не готовые ключи, а сгенерированная центром распределения ключей предварительная ключевая информация – секретные данные меньшего объема, с помощью которых каждое устройство может самостоятельно вычислить общий секретный ключ;

2) протоколы передачи сгенерированных ключей;

3) протоколы совместной выработки общего ключа, т.е. открытое распределение ключей.

В работе протоколов распределения ключей можно выделить три этапа [5].

1. Во время этапа *инициализации* каждый участник системы получает предварительную информацию (секретную и публичную части), необходимую для дальнейшей работы схемы, от доверенного центра или администратора сети.

2. Этап *организации общего секретного ключа*, во время которого группа пользователей системы с помощью заранее оговоренного алгоритма, используя полученную на этапе инициализации предварительную информацию, вычисляет общий секретный ключ. Этот этап повторяется каждый раз, когда группе участников протокола требуется общий секретный ключ. Отметим, что в разных типах протоколов используют различные алгоритмы, и именно используемый алгоритм в основном определяет характеристики схемы, а также - какая предварительная ключевая информация должна раздаваться на этапе инициализации.

3. Этап *обновления* может происходить по нескольким причинам, таким как: изменение структуры сети, например, в результате добавления новых или исключения существующих пользователей; изменение состава групп, которые могут организовывать общие секретные ключи; необходимость обновления ключевой информации по причине истечения времени жизни ключей.

Отметим, что этап обновления не является обязательным и его можно рассматривать как начальную инициализацию новой схемы, поэтому в дальнейшем внимание будет уделяться только этапам инициализации и организации общего секретного ключа.

Рассмотрим подробнее типы протоколов организации ключей.

1. Схемы предварительного распределения ключей. В протоколах этого типа на этапе организации общего секретного ключа не предполагается возможность какой-либо коммуникации между участниками системы или с доверенным центром. Доверенный центр или администратор участвует только на этапе инициализации, когда он распределяет между пользователями системы предварительную ключевую информацию. Затем каждый участник может независимо от других участников без какого-либо дополнительного обмена сообщениями и только на основе предварительной ключевой информации вычислить общие секретные ключи для любой предусмотренной протоколом группы с его участием. Таким образом, вся предварительная ключевая информация, а следовательно, и все общие секретные ключи в системе, полностью зависят от доверенного сервера. Примерами таких схем являются полилинейные системы [6,7] и комбинаторные системы [8].

2. Протоколы передачи сгенерированных ключей. В таких протоколах генерацией и распределением ключей чаще всего занимается некоторый доверенный центр. При этом в отличие от схем предварительного распределения ключей доверенный центр остается доступным и после завершения этапа инициализации, поэтому на этапе организации общего секретного ключа участники могут обмениваться с ним сообщениями, а генерация и передача результирующих секретных ключей может происходить по запросу участника протокола, а не заранее, как в предыдущем случае.

3. Протоколы совместной выработки общего ключа. В системах такого типа, как и в схемах предварительного распределения ключей, доверенный сервер становится недоступным после этапа инициализации, но при этом пользователи системы имеют возможность обмена сообщениями друг с другом по открытым каналам связи на этапе организации ключей. К таким схемам, например, относится протокол Диффи-Хэллмана и различные его вариации.

Можно сделать следующие выводы о рассмотренных выше подходах к решению задачи организации общих секретных ключей применительно к беспровод-

ным сенсорным сетям. Протоколы передачи сгенерированных ключей плохо согласуются с беспроводными сенсорными сетями, т.к. после запуска сети доверенный центр, как правило, не доступен для сенсоров. Протоколы совместной выработки общего ключа также не подходят для маломощных сенсоров с ограниченным источником питания, т.к. из-за применения тяжелых алгоритмов криптографии с открытым ключом и необходимого для них дополнительного обмена сообщениями они потребуют дополнительных вычислительных и энергетических затрат. Поэтому для беспроводных сенсорных сетей наиболее целесообразным представляются использование схем предварительного распределения ключей.

2. Модель организации защищенной связи в беспроводной сенсорной сети на основе предварительного распределения ключей, обеспечивающая защиту от внешнего злоумышленника

Для связи друг с другом сенсоры используют беспроводные каналы связи. Передаваемые в них данные могут быть довольно легко перехвачены внешним наблюдателем. Схемы предварительного распределения ключей обеспечивают стороны передачи данных общим секретным ключом, который позволяет защитить передаваемые данные от внешнего злоумышленника. Но т.к. беспроводная сенсорная сеть может быть размещена в условиях, при которых доступ к самим устройствам не может строго контролироваться, то также возникает проблема внутреннего злоумышленника, который может получить доступ к некоторым устройствам сети и извлечь их секретную ключевую информацию. Полученную секретную ключевую информацию он затем может попытаться использовать для того, чтобы вычислить общие секретные ключи, используемые другими сенсорами в сети. Поэтому протоколы распределения ключей должны также учитывать возможное присутствие внутреннего злоумышленника.

Рассмотрим сначала модель схемы предварительного распределения ключей для сети X, предназначенной для обеспечения защиты от внешнего злоумышленника.

На этапе инициализации доверенный центр выбирает предварительное ключевое пространство K, множество идентификаторов I ключей из K и инъективное отображение $\mathrm{iden}: K \to I$, с помощью которого каждому ключу ставится в соответствие идентификатор $i = \mathrm{iden}(k)$. Таким образом, можно сравнить, являются ли два ключа одинаковыми, проверив на равенство их идентификаторы. Причем функция iden известна только доверенному центру и выбирается таким образом, чтобы по значению идентификатора i невозможно восстановить соответствующий ему ключ k. Пусть

$$KI = K \times I = \{(k,i) | k \in K, i \in I\}$$

Каждому устройству $x \in X$ доверенный центр передает предварительную ключевую информацию

$$KI_x = \{(k_{x,j}, i_{x,j}), k_{x,j} \in K, i_{x,j} \in I, i_{x,j} = \mathrm{iden}(k_{x,j}), j = 1..|KI_x|\} \subset KI,$$

состоящую из секретных ключей и соответствующих им идентификаторов. Для удобства введем также множество $K_x = \{k_{x,j}\} \subset K$, состоящее только из секретных ключей устройства x, и множество $I_x = \{i_{x,j}\} \subset I$, состоящее только из соответствующих этим ключам идентификаторов. Множество I_x является публичной информацией устройства x. Имеющиеся у x секретные ключи определяют, с какими другими устройствами в сети он сможет обмениваться данными, поэтому множество I_x может также использоваться в качестве идентификатора устройства x.

В дальнейшем для простоты будем считать, что передача данных может осуществляться только в группах из двух устройств.

На этапе организации ключа для обеспечения безопасности передачи данных между устройствами, участникам нужно иметь общий секретный ключ из некоторого ключевого пространства Ω. Для этого имеется известный всем участникам системы алгоритм вычисления общего секретного ключа

$$\gamma: 2^{KI} \times 2^{I} \to \Omega \cup \{\perp\}, \quad (1)$$

для которого

$$\forall x, y \in X, x \neq y, \gamma(KI_x, I_y) = \gamma(KI_y, I_x). \quad (2)$$

С помощью γ каждый сенсор x на основе своей предварительной ключевой информацией KI_x и публичной части I_y ключевой информации сенсора y может вычислить общий секретный ключ $\omega_{x,y} = \gamma(KI_x, I_y)$ в случае, когда $\gamma(KI_x, I_y) \in \Omega$. Выполнение равенства $\gamma(KI_x, I_y) = \perp$ означает, что в системе не предусмотрена группа $\{x, y\}$, а значит, у x нет возможности напрямую передать данные устройству y. Выполнение условия (2) обеспечивает, что оба участника группы $\{x, y\}$ смогут вычислить один и тот же общий секретный ключ.

Выше было отмечено, что протоколы распределения ключей разрабатываются в первую очередь для обеспечения безопасности от внешнего наблюдателя. Рассмотрим условия, которые должны выполняться для того, чтобы описанная схема предоставляла такую защиту. Предполагается, что внешнему наблюдателю известна публичная часть предварительной ключевой информации I_x для каждого сенсора x, но не известны соответствующие K_x. Поэтому алгоритм γ вычисления общего секретного ключа $\omega_{x,y}$ (см. (1)) должен быть таким, чтобы его результат нельзя было предсказать на основе публичной информации I_x и I_y, а именно, чтобы энтропия (степень неопределенности) ключа $\omega_{x,y}$ при известных I_x и I_y совпадала с энтропией этого ключа при неизвестных I_x и I_y:

DOI:10.21681/2311-3456-2020-03-13-21

$$H(\omega_{x,y}) = H(\omega_{x,y}|I_x, I_y)$$

т.е. энтропия $\omega_{x,y}$ зависит от секретной части ключевой информации. Другими словами, в этой ситуации внешний злоумышленник не получит никакой информации о ключе $\omega_{x,y}$ из идентификаторов I_x и I_y. Далее предполагается, что для обеспечения устойчивости криптосистемы, в которой используется полученный общий секретный ключ, требуется, чтобы

$$H(\omega_{x,y}) \geq H_\Omega \qquad (3)$$

для некоторого значения H_Ω.

Рассмотрим несколько простых примеров схем предварительного распределения ключей, удовлетворяющих этим условиям.

Пример 1. Рассмотрим следующую простую схему предварительного распределения ключей на множестве устройств X ($|X| = n$), в которой каждое устройство x в качестве своей секретной информации $K_x = \{\omega_{x,y} \in \Omega : y \in X \backslash \{x\}\}$ получает набор общих секретных ключей $\omega_{x,y}$ для каждого из y, а в качестве открытой – $I_x = \{\{x, y\} : y \in X\{x\}\}$, идентифицирующее устройство x. Функция γ по идентификатору I_y выбирает из набора K_x общий секретный ключ $\omega_{x,y} = \gamma(KI_x, I_y)$ для группы $\{x, y\}$. В этом случае злоумышленник, зная только идентификаторы I_x и I_y не сможет узнать их общий секретный ключ. Проблемой такой схемы является то, что объем секретной информации K_x, содержащей все общие секретные ключи для передачи данных между x и любым другим устройством y, будет слишком большим при большом количестве устройств в сети. В данном примере предварительное ключевое множество K и множество Ω совпадают, и в качестве общего секретного ключа используется один из предварительных ключей. Поэтому для того, чтобы выполнялось условие (3), энтропия предварительного ключа должна быть не меньше H_Ω, а значит каждому устройству в сети потребуется хранить по крайней мере $M_x = H_\Omega \cdot (n-1)$ байт предварительной ключевой информации.

Пример 2. В другой возможной схеме предварительного распределения ключей каждое устройство x в качестве секретной информации K_x получает один и тот же общий секретный ключ k, который будет использоваться для всех возможных групп в сети. Функция γ в этом случае будет выглядеть следующим образом: $\gamma(KI_x, I_y) = k$. В такой схеме объем секретной информации K_x, которую нужно будет хранить каждому устройству в сети, будет мал, и при этом внешний злоумышленник все еще не может получить общий секретный ключ никакой из возможных групп, не зная значения K_x. В этой схеме для того, чтобы выполнялось условие (3), каждому устройству в сети понадобится хранить $M_x = H_\Omega$ байт предварительной ключевой информации.

В примере 2 каждому устройству требуется хранить всего лишь один ключ, в то время как в примере 1 каждому устройству понадобится хранить $n-1$ ключей. Однако в случае наличия внутреннего злоумышленника, который сможет получить доступ к одному из устройств, схема из примера 2 будет сразу же скомпрометирована – злоумышленник сможет получить доступ сразу ко всем возможным группам внутри сети. В схеме из примера 1 при компрометации одного из предварительных ключей злоумышленник сможет получить доступ лишь к тем данным, которые предаются между двумя сенсорами, использующими этот ключ, а в случае компрометации всех предварительных ключей одного сенсора – только к данным, передающимся с участием этого сенсора.

3. Схемы предварительного распределения ключей, обеспечивающие защиту от внешнего и внутреннего злоумышленников

Из проведенного выше анализа вытекает, что имеются две основные проблемы, возникающие при построении схем предварительного распределения ключей. Во-первых, внутренний злоумышленник не должен получить значительную часть секретных ключей, используемых в системе, даже в случае компрометации им нескольких устройств. Во-вторых, т.к. память сенсоров является ограниченным ресурсом, то объем предварительной ключевой информации не должен быть слишком большим. Для решения этих проблем разрабатываются новые и совершенствуются известные подходы (см. [9]).

Один из таких подходов – *вероятностные схемы* – был предложен в [10]. В схемах такого типа каждое устройство случайным образом получает часть ключей из набора предварительных секретных ключей, сгенерированных для системы. Если в результате распределения у двух узлов сети среди их предварительных ключей найдутся одинаковые, то с их помощью они смогут получить общий секретный ключ. Но из-за случайного распределения ключей у некоторых пар сенсоров может не оказаться общих предварительных ключей, а значит, они не смогут напрямую обмениваться данными. Таким образом, уменьшается связность сети, что является основным минусом таких схем. Отметим, что связность сети может регулироваться изменением доли предварительных ключей, которую получает каждое устройство, т.к. при ее увеличении увеличивается и вероятность того, что у пары сенсоров окажутся общие ключи. Но при этом увеличивается как объем предварительной ключевой информации, которую потребуется хранить каждому сенсору, так и вероятность того, что внутренний злоумышленник в результате компрометации одного из устройств получит все предварительные ключи, общие для других сенсоров.

Два других подхода к построению схем предварительного распределения ключей – *комбинаторные схемы* и *полилинейные схемы*. Одним из способов построения комбинаторных схем является использование шаблонов распределения ключей, предложенных в [11]. Примерами таких схем являются схема [12], построенная на комбинаторных дизайнах, и схема [13] на основе ортогональных массивов. Полилинейные схемы были предложены в [14,15], а затем они были обобще-

ны В. Сидельниковым в [16]. В отличие от вероятностных схем в комбинаторных и полилинейных схемах предварительная ключевая информация распределяется детерминировано; в случае комбинаторных схем это делается в соответствии с некоторой комбинаторной структурой, а полилинейные схемы могут строиться на основе помехоустойчивых кодов. Такие подходы позволяют получать схемы с более предсказуемыми свойствами. В частности, в таких схемах группы устройств, способные организовывать общие секретные ключи, могут задаваться заранее, из-за чего связность в сети больше не зависит от случайного распределения предварительной ключевой информации. При этом для обеспечения наилучшей связности нередко разрабатываются схемы, в которых любой сенсор может получить общий секретный ключ для передачи данных любому другому устройству в сети.

Среди множества комбинаторных и полилинейных схем можно выделить такие, которые относятся к *пороговым* схемам. Они обладают тем свойством, что гарантируют безопасность общих секретных ключей, если размер коалиции сенсоров, скомпрометированных внутренним злоумышленником, не превышает некоторого заданного в системе порога. В этом случае злоумышленник сможет получить только общие секретные ключи, используемые сенсорами из коалиции. Однако в случае, когда размер коалиции превышает предусмотренный в системе порог, безопасность ключей больше не гарантируется. При этом в зависимости от построения системы это может означать, как то, что злоумышленник получит все общие ключи в системе, так и то, что он сможет получить только какую-то, возможно небольшую, долю ключей, используемых сенсорами, не входящими в его коалицию. Тогда возникает задача оценки этой доли или, другими словами, оценки вероятности того, что случайно сформированная коалиция внутреннего злоумышленника может получить общие секретные ключи, используемые для передачи данных произвольной парой нескомпрометированных устройств в системе.

Таким образом, для борьбы с коалиционными атаками, проводимыми внутренним злоумышленником, представляется целесообразным использовать пороговые схемы предварительного распределения ключей с предварительным вычислением вероятности успешного проведения коалиционных атак.

Ниже рассмотрим подробнее примеры пороговых схем предварительного распределения ключей, а именно комбинаторную схему, построенную на основе дизайнов Адамара [8], и полилинейную схему, построенную на основе кодов Рида-Маллера [7].

Замечание. Разрабатываются также схемы, которые объединяют идеи из этих основных подходов. Так, например, в [17] совмещаются вероятностный и комбинаторный подходы. Предложенная в [18] схема представляет из себя несколько полилинейных схем, при этом, в каких схемах участвует каждое устройство в сети, выбирается случайным образом. В [19] строится иерархическая система, на каждом уровне которой используется своя схема предварительного распределения ключей.

3.1. Модель комбинаторной схемы предварительного распределения ключей, основанной на дизайнах Адамара

Рассмотрим комбинаторную схему, построенную на основе дизайнов Адамара, ранее исследованную в [8]. В такой схеме для $n = 2^a$ устройств доверенный центр генерирует дизайн Адамара [20], представляющий из себя множество из n точек и множество $2(n-1)$ блоков – подмножеств множества точек. Для каждого блока дизайна доверенный центр генерирует ключ $k_i \in K$. Каждой точке дизайна ставится в соответствие устройство сети $x \in X$, которое получает в качестве секретной ключевой информации все ключи, соответствующие блокам, в которые входит эта точка. Таким образом, по свойствам дизайна Адамара каждое устройство получает $n-1$ ключ, и каждый ключ оказывается у $n/2$ устройств. При этом у каждой пары устройств имеется $n/2-1$ общих ключей, на основе которых они могут вычислить общий секретный ключ. Отсюда вытекает, что для того, чтобы получившийся ключ был основан на H_Ω байт секретной ключевой информации, размер каждого предварительного ключа должен быть не менее $H_K = \frac{H_\Omega}{n/2-1}$. Таким образом, каждому устройству понадобится хранить по крайней мере $M_x = \frac{H_\Omega}{n/2-1}(n-1) \approx 2H_\Omega$ байт предварительной ключевой информации.

В такой системе внешний злоумышленник, зная только публичные идентификаторы устройств, так же не получает никакой информации об общих секретных ключах. В случае компрометации одного из предварительных ключей, энтропия общего секретного ключа несколько уменьшится, т.к. он будет создан с использованием $H_\Omega - H_K = \frac{n-4}{n-2}H_\Omega$ секретных байт.

Однако ситуация, когда будет скомпрометирован только один из предварительных ключей, представляется маловероятной, т.к. скорее всего внутренний злоумышленник сразу получит всю предварительную ключевую информацию одного из устройств сети. В этом случае по свойствам дизайна Адамара он получит $n/4-1$ из общих предварительных ключей двух устройств, а значит их общий секретный ключ будет основан всего на $\frac{H_\Omega}{2(1-2/n)}$ секретных байт. Поэтому если предполагается, что одно из устройств сети может быть скомпрометировано, то можно вместо этого использовать предварительные ключи размером не менее $H_K = 4H_\Omega/n$ байт. Суммарный объем предварительной ключевой информации, которою должно будет хра-

нить каждое устройство, в этом случае будет не менее $4H_\Omega$ байт.

В случае же, если внутренний злоумышленник получил доступ к двум устройствам в сети, то ему будет не хватать только одного из предварительных ключей для того, чтобы вычислить общий секретный ключ какой-то пары сенсоров. Поэтому для обеспечения безопасности передачи данных каждый предварительный ключ должен будет иметь размер не менее H_Ω, , а для хранения всей предварительной ключевой информации сенсору понадобится по крайней мере $(n-1)H_\Omega$ байт памяти. Таким образом, в случае, если предполагается возможность компрометации внутренним злоумышленником двух устройств в сети, то такая схема может гарантировать защиту общих секретных ключей, но объем предварительной ключевой информации, которую потребуется хранить каждому сенсору будет таким же, как в примере 1.

В случае, если внутренний злоумышленник получил предварительную ключевую информацию с трех и более устройств сети, то в объединении ключевой информации с этих устройств будут находиться все предварительные секретные ключи одного или нескольких других сенсоров, не входящих в коалицию. Тогда с их помощью злоумышленник сможет вычислить любой общий секретный ключ, который используется одним из этих устройств. Вероятность того, что внутренний злоумышленник получит общий секретный ключ произвольной пары сенсоров в результате компрометации w устройств в сети, может быть вычислена по формуле [8]

$$p(w) = \\ = \sum_{r=1}^{w} \frac{C_2^1 {}_{r-1-w} \cdot C_{n-2}^1 {}_{r-1} + C_2^2 {}_{r-1-w}}{C_n^2} p(B(w,r)), \quad (4)$$

где $p\left(B\left(w,r\right)\right)$ вычисляется рекуррентно:

$$p\left(B(w,r)\right) = \\ = \frac{p\left(B(w-1,r-1)\right)\cdot\left(n-2^{r-2}\right)+p\left(B(w-1,r)\right)\cdot\left(2^{r-1}-w+1\right)}{n-w+1}, \quad (5)$$

$$p\left(B(1,1)\right) = 1; p\left(B(w,0)\right) = 0; \\ p\left(B(1,r)\right) = 0, r \neq 1. \quad (6)$$

При этом для того, чтобы иметь возможность вычислить общие секретные ключи всех сенсоров в системе, как в примере 2, внутреннему злоумышленнику в лучшем для него случае понадобится получить предварительную ключевую информацию с $\log_2 n$ устройств в сети, а в худшем – с $n/2+1$ устройств.

Таким образом, в зависимости от того, к какому количеству устройств внутренний злоумышленник сможет потенциально получить доступ, схема распределения ключей на основе дизайна Адамара может настраиваться: в случае, если внутренний злоумышленник не сможет скомпрометировать более одного устройства, то можно значительно уменьшить объем хранимой предварительной ключевой информации без ущерба безопасности системы.

3.2. Модель полилинейной схемы предварительного распределения ключей

Рассмотрим полилинейную систему распределения ключей для передачи данных между двумя участниками, построенную на основе двоичных кодов Рида-Маллера порядка $m-2$, которая ранее была описана в [7]. Для сети X из $|X| = n = 2^m$ устройств доверенный центр генерирует проверочную матрицу двоичного кода Рида-Маллера порядка $m-2$ (или, что то же самое, порождающую матрицу двоичного кода Рида-Маллера порядка 1) размера $(m+1)\times 2^m$. Каждый столбец матрицы ставится в соответствие одному устройству в сети, обозначим его x_j. В качестве предварительного ключевого пространства K доверенный центр выбирает линейное векторное пространство $\mathbb{F}_2^u$, при этом u выбирается много больше $C_{m+2}^2 = (m+1)(m+2)/2$. Во множестве K доверенный центр фиксирует подпространство размерности $(m+1)(m+2)/2$ и выбирает в нем базис $\Xi = \{\xi_{i_1,i_2} \in K | 1 \le i_1 \le i_2 \le m+1\}$. На основе этих векторов для каждого устройства x_j доверенный центр вычисляет множество $\Xi(x_j) = \{\xi_i(x_j) | 1 \le i \le m+1\}$, где каждый $\xi_i(x_j)$ является линейной комбинацией исходных векторов из Ξ с коэффициентами, определяемыми соответствующим столбцом проверочной матрицы. Множество $\Xi(\mathrm{x_j})$ является секретной частью предварительной ключевой информации сенсора x_j, а соответствующий ему вектор-столбец проверочной матрицы – его идентификатором, открытой информацией. Отметим, что множество $\Xi(\mathrm{x_j})$ состоит из $|\Xi(x_j)| = m+1$ векторов.

Сенсор x на основе своей секретной предварительной ключевой информации $\Xi(x)$ и векторов-столбов, соответствующих сенсорам x и y может вычислить общий секретный ключ для передачи данных с устройством y. Общий секретный ключ вычисляется как линейная комбинация векторов из $\Xi(x)$ с коэффициентами, определяемыми векторами x и y. Таким образом, общий секретный ключ также является вектором пространства K. Для того, чтобы выполнялось условие (3), энтропия ключей из K должна быть больше H_Ω, что обеспечивается достаточно большой размерностью u. В этом случае каждому сенсору нужно будет хранить $(m+1)H_\Omega = (\log_2 n + 1)H_\Omega$ байт предварительной ключевой информации, что значительно меньше, чем требовалось в предыдущих рассмотренных примерах.

При этом такая схема предварительного распределения ключей, построенная на кодах Рида-Маллера, гарантирует безопасность общих секретных ключей при наличии коалиции внутренних злоумышленников

размера не более чем два. В этом случае описанные в [16] полилинейные схемы обеспечивают совершенную секретность ключей, т.е. внутренний злоумышленник на основе предварительной ключевой информации со скомпрометированных устройств не получает никакой информации об общих секретных ключах, используемых другими устройствами в сети. Однако в случае превышения допустимого размера коалиции внутренний злоумышленник получит возможность вычислить приватную ключевую информацию одного или нескольких устройств в сети и с помощью нее сможет получить все общие секретные ключи, используемые этими устройствами. Так как дизайны Адамара и коды Рида-Маллера порядка 1 обладают схожими свойствами, то вероятность того, что внутренний злоумышленник получит общий секретный ключ произвольной пары сенсоров в результате компрометации w устройств в сети, также может быть вычислена по формулам (4-6) [7]. Но в случае, если система строится на основе других кодов, то эта вероятность может значительно отличаться. Так, например, в случае использования кодов Рида-Соломона, при превышении размера коалиции хотя бы на одно устройство схема больше не обеспечивает никакой защиты, т.к. внутренний злоумышленник сможет вычислить все используемые в системе общие ключи. Однако при этом в такой схеме каждому устройству потребуется хранить минимально возможное число предварительных ключей [16].

Выводы

В работе проанализированы существующие типы протоколов организации секретных ключей в беспроводных сенсорных сетях и наиболее подходящими выбраны схемы предварительного распределения ключей. Выделены две основные проблемы, возникающие при проектировании таких схем, рассмотрены подходы к построению схем, учитывающие эти проблемы, выделены существенные особенности, которые следует учитывать при выборе схемы.

Наиболее подходящими схемами представляются пороговые полилинейные и близкие к ним комбинаторные схемы, которые благодаря тому, что используют предварительную ключевую информацию меньшего объема, а также обеспечивают защиту от коалиций небольшой мощности, могут использоваться в случаях, когда объем доступной памяти устройств сильно ограничен и предполагается наличие внутреннего злоумышленника. Правильность полученных выводов подтверждается проведенными ранее исследованиями авторов [6-8].

Литература

1. Гольдштейн Б.С., Кучерявый А.Е. Сети связи пост-NGN. СПб.: БХВ-Петербург, 2013.160 с.
2. Karlof C., Wagner D. Secure routing in wireless sensor networks: attacks and countermeasures. // Ad Hoc Networks, Volume 1, Issues 2-3, September 2003, pp. 293-315. DOI: 10.1016/S1570-8705(03)00008-8
3. Al-Karaki J.N. and Kamal A.E. Routing techniques in wireless sensor networks: A survey. // IEEE Wireless Communications Magazine, vol. 11, no. 6, 2004, pp. 6-28. DOI: 10.1109/MWC.2004.1368893
4. Словарь криптографических терминов. / под ред. Б.А. Погорелова и В.Н. Сачкова. М.: МЦНМО. 2006. 94 с.
5. Martin K.M. The Combinatorics of Cryptographic Key Establishment / Surveys in Combinatorics (London Mathematical Society Lecture Note Series), 2007, pp. 223-273. DOI: 10.1017/CBO9780511666209.009
6. Деундяк В.М., Таран А.А. О применении кодов Хэмминга в системе распределения ключей для конференций в многопользовательских системах связи // Вестник ВГУ. Серия: Системный анализ и информационные технологии. 2015. № 3. С. 43-50.
7. Деундяк В.М., Таран А.А. О вероятности проведения успешных атак на ключи конференций в полилинейных системах распределения ключей // Известия вузов. Северо-Кавк. Регион. Техн. Науки. 2018. № 1. С. 10-17.
8. Деундяк В.М., Таран А.А. Система распределения ключей на дизайнах Адамара // Моделирование и анализ информационных систем. 2019. 26(2). С. 229-243. DOI: 10.18255/1818-1015-2019-2-229-243
9. Martin K.M., Paterson M. An Application-Oriented Framework for Wireless Sensor Network Key Establishment. // Electronic Notes in Theoretical Computer Science, vol. 192(2), 2008, pp. 31-41. DOI: 10.1016/j.entcs.2008.05.004
10. Eschenauer L., Gligor. V.D. A key-management scheme for distributed sensor networks. // CCS '02: Proceedings of the 9th ACM conference on Computer and communications security, 2002, pp. 41–47. DOI: 10.1145/586110.586117
11. Mitchell C.J., Piper F.C. Key Storage in Secure Networks. // Discrete Applied Mathematics, vol. 21(3), 1988, pp. 215–228. DOI: 10.1016/0166-218X(88)90068-6
12. Stinson D.R. On Some Methods for Unconditionally Secure Key Distribution and Broadcast Encryption. // Designs, Codes and Cryptograpy, 1997, pp. 215–243. DOI: 10.1023/A:1008268610932
13. Stinson D.R., Trung T.V. Some New Results on Key Distribution Patterns and Broadcast Encryption. // Designs, Codes and Cryptography, 1998, pp. 261–279. DOI: 10.1023/A:1008209004667
14. Blom R. An Optimal Class of Symmetric Key Generation Systems // Workshop on the Theory and Applications of Cryptographic Techniques, 1985, pp. 335–338. DOI: 10.1007/3-540-39757-4_22
15. Blundo C., Mattos L.A.F., Stinson D.R. Trade-offs Between Communication and Storage in Unconditionally Secure Schemes for Broadcast Encryption and Interactive Key Distribution // Annual International Cryptography Conference, 1996, pp. 387–400. DOI: 10.1007/3-540-68697-5_29
16. Сидельников В.М. Теория кодирования. М.: ФИЗМАТЛИТ. 2008. 324 с.

17. Liu D., Ning P. Establishing pairwise keys in distributed sensor networks. // CCS '03: Proceedings of the 10th ACM conference on Computer and communications security, 2003, pp. 52–61. DOI: 10.1145/948109.948119
18. Du W., Deng J., Han Y., Varshney P. A pairwise key pre-distribution scheme for wireless sensor networks. // CCS '03: Proceedings of the 10th ACM conference on Computer and communications security, 2003, pp. 42–51. DOI: 10.1145/948109.948118
19. Mohaisen A., Nyang D., Lee K. Hierarchical Grid-based Pairwise KeyPre-distribution in Wireless Sensor Networks // International Journal of Network Security, vol. 8(3), 2009, pp. 282–292.
20. Таранников Ю.В. Комбинаторные свойства дискретных структур и приложения к криптологии. М.:МЦНМО. 2011. 152 с.

Рецензент: *Петренко Сергей Анатольевич, доктор технических наук, профессор, руководитель Центра информационной безопасности Университета Иннополис, Иннополис, Россия. E-mail: s.petrenko@rambler.ru*

ON THE PROBLEM OF SECURE COMMUNICATION IN WIRELESS SENSOR NETWORKS

Deundyak V.M.[3], Taran A.A.[4]

Abstract. *The goal of the paper is a secure communication in wireless sensor networks in the presence of external and internal attackers. Comparative analysis of different types of key distribution protocols is performed, different approaches to building secure communication schemes in wireless sensor networks are studied, and estimations for the entropy of the predistributed key information are calculated. The key predistribution schemes are suggested to be used for wireless sensor networks; the model of such schemes that provide protection from external attacker is developed. The requirements to the size of predistributed key information for each device in the network are studied based on the requirements to common secret key and scheme resilience against collusive attacks by internal attacker. For better resilience against collusive attacks threshold key predistribution schemes such as polylinear and combinatorial schemes are suggested to be used. Probabilities of successful attacks in case when size of the coalition exceeds the threshold are studied for such schemes. The conclusions are supported by previously conducted research.*

Keywords: *wireless sensor networks, secret key establishment, key predistribution schemes, threshold schemes, polylinear schemes, combinatorial schemes, collusive attacks.*

References

1. Gol'dshteyn B.S., Kucheryavyy A.E. Seti svyazi post-NGN. – Saint-Petersburg: BKhV-Peterburg, 2013, 160 p.
2. Karlof C., Wagner D. Secure routing in wireless sensor networks: attacks and countermeasures. // Ad Hoc Networks, Volume 1, Issues 2-3, September 2003, pp. 293-315. DOI: 10.1016/S1570-8705(03)00008-8
3. Al-Karaki J.N. and Kamal A.E. Routing techniques in wireless sensor networks: A survey. // IEEE Wireless Communications Magazine, vol. 11, no. 6, 2004, pp. 6-28. DOI: 10.1109/MWC.2004.1368893
4. Slovar' kriptograficheskikh terminov. / by ed. B.A. Pogorelov and V.N. Sachkov. Moskow: MTsNMO, 2006, 94 p.
5. Martin K.M. The Combinatorics of Cryptographic Key Establishment / Surveys in Combinatorics (London Mathematical Society Lecture Note Series), 2007, pp. 223-273. DOI: 10.1017/CBO9780511666209.009
6. Deundyak V.M., Taran A.A. O primenenii kodov Khemminga v sisteme raspredeleniya klyuchey dlya konferentsiy v mnogopol'zovatel'skikh sistemakh svyazi // Vestnik VGU. Seriya: Sistemnyy analiz i informatsionnye tekhnologii, 2015, № 3, pp. 43-50.
7. Deundyak V.M., Taran A.A. O veroyatnosti provedeniya uspeshnykh atak na klyuchi konferentsiy v polilineynykh sistemakh raspredeleniya klyuchey // Izvestiya vuzov. Severo-Kavk. Region. Tekhn. nauki, 2018, № 1, pp. 10-17.
8. Deundyak V.M., Taran A.A. Sistema raspredeleniya klyuchey na dizaynakh Adamara // Modelirovanie i analiz informatsionnykh sistem, 2019, 26(2), pp. 229-243. https://doi.org/10.18255/1818-1015-2019-2-229-243
9. Martin K.M., Paterson M. An Application-Oriented Framework for Wireless Sensor Network Key Establishment. // Electronic Notes in Theoretical Computer Science, vol. 192(2), 2008, pp. 31-41. DOI: 10.1016/j.entcs.2008.05.004
10. Eschenauer L., Gligor. V.D. A key-management scheme for distributed sensor networks. // CCS '02: Proceedings of the 9th ACM conference on Computer and communications security, 2002, pp. 41–47. DOI: 10.1145/586110.586117

3 Vladimir Deundyak, Ph.D., Associate Professor, Southern Federal University, FGNU NII «Specvuzavtomatika», Rostov-on-Don, Russia. ORCID: orcid.org/0000-0001-8258-2419. E-mail: vl.deundyak@gmail.com

4 Alexey Taran, graduate student, Southern Federal University, Rostov-on-Don, Russia. ORCID: orcid.org/0000-0002-1357-9360. E-mail: fraktal-at@yandex.ru

11. Mitchell C.J., Piper F.C. Key Storage in Secure Networks. // Discrete Applied Mathematics, vol. 21(3), 1988, pp. 215–228. DOI: 10.1016/0166-218X(88)90068-6
12. Stinson D.R. On Some Methods for Unconditionally Secure Key Distribution and Broadcast Encryption. // Designs, Codes and Cryptograpy, 1997, pp. 215–243. DOI: 10.1023/A:1008268610932
13. Stinson D.R., Trung T.V. Some New Results on Key Distribution Patterns and Broadcast Encryption. // Designs, Codes and Cryptography, 1998, pp. 261–279. DOI: 10.1023/A:1008209004667
14. Blom R. An Optimal Class of Symmetric Key Generation Systems // Workshop on the Theory and Applications of Cryptographic Techniques, 1985, pp. 335–338. DOI: 10.1007/3-540-39757-4_22
15. Blundo C., Mattos L.A.F., Stinson D.R. Trade-offs Between Communication and Storage in Unconditionally Secure Schemes for Broadcast Encryption and Interactive Key Distribution // Annual International Cryptography Conference, 1996, pp. 387–400. DOI: 10.1007/3-540-68697-5_29
16. Sidel'nikov V.M. Teoriya kodirovaniya – Moskow: FIZMATLIT, 2008, 324 p.
17. Liu D., Ning P. Establishing pairwise keys in distributed sensor networks. // CCS '03: Proceedings of the 10th ACM conference on Computer and communications security, 2003, pp. 52–61. DOI: 10.1145/948109.948119
18. Du W., Deng J., Han Y., Varshney P. A pairwise key pre-distribution scheme for wireless sensor networks. // CCS '03: Proceedings of the 10th ACM conference on Computer and communications security, 2003, pp. 42–51. DOI: 10.1145/948109.948118
19. Mohaisen A., Nyang D., Lee K. Hierarchical Grid-based Pairwise KeyPre-distribution in Wireless Sensor Networks // International Journal of Network Security, vol. 8(3), 2009, pp. 282–292.
20. Tarannikov Yu.V. Kombinatornye svoystva diskretnykh struktur i prilozheniya k kriptologii – Moskow: MTsNMO, 2011, 152 p.