УДК 004.056 **DOI** 10.15622/sp.2019.18.3.705-740

В.А. Яковлев

АУТЕНТИФИКАЦИЯ КЛЮЧЕЙ, РАСПРЕДЕЛЯЕМЫХ МЕТОДОМ ДИФФИ — ХЕЛЛМАНА, ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ НА ОСНОВЕ АУТЕНТИФИЦИРУЮЩИХ ПОМЕХОУСТОЙЧИВЫХ КОДОВ И МАГНИТОМЕТРИЧЕСКИХ ДАННЫХ

Яковлев В.А. **Аутентификация ключей, распределяемых методом Диффи — Хеллмана, для мобильных устройств на основе аутентифицирующих помехоустойчивых кодов и магнитометрических данных.**

Аннотация. Широкое распространение мобильных беспроводных устройств (смартфонов, планшетов и пр.) остро ставит вопрос о криптографической защите передаваемой этими устройствами информации, что, в свою очередь, требует обеспечения этих устройств ключами, а также решения задачи их аутентификации. В последнее время актуализировались исследования способов аутентификации ключей в рамках сценария сопряжения (спаривания) мобильных устройств. В этих условиях мобильные устройства располагаются близко друг к другу, вплоть до физического контакта, и между ними создается защищенный от перехвата дополнительный канал обмена данными с целью аутентификации ключей.

Анализ дополнительных каналов — визуального, акустического, вибрационного, тактильного, магнитометрического — выявил преимущества последнего по скорости и достоверности аутентификации, а также удобству использования этого канала по сравнению с другими способами. Магнитометрический канал образуется при наличии в мобильных устройствах магнитометров, измеряющих магнитное поле Земли. Случайные колебания магнитного поля в точке измерения позволяют получить в двух мобильных устройствах совпадающие с большой вероятностью случайные последовательности, которые могут быть использованы для аутентификации сеансовых ключей.

В статье исследуется протокол под названием Magparing, который предназначен для аутентификации ключей мобильных устройств, распределяемых по методу Диффи — Хеллмана, на основе использования показаний магнитометров этих устройств. Детальный анализ этого протокола показал его уязвимость к атаке «человек-посередине». Уязвимость протокола также подтверждена с помощью программы анализа безопасности протоколов AVISPA.

Предложен безопасный способ аутентификации ключей (значений Диффи — Хеллмана) на основе аутентифицирующих помехоустойчивых кодов (АП-кодов). Аутентификаторы для значений Диффи — Хеллмана формируются на основе блоков АП-кода и случайных последовательностей, полученных из показаний магнитометров. Предложен подход к оптимизации параметров АП-кода, обеспечивающего21 выполнение требований по вероятности ложного отклонения и вероятности навязывания ключа заданной длины при минимизации длины цепочки магнитометрических данных, расходуемых в процедуре аутентификации. Приведен пример выбора параметров кода для аутентификации ключа длиной 256 бит, обеспечивающего вероятностью навязывания ложного ключа не более 10^{-9} при вероятности ложного отклонения истинного ключа -10^{-6}, что свидетельствует о реализуемости этого способа аутентификации.

Ключевые слова: аутентификация, распределение ключей, метод Диффи — Хеллмана, дополнительный канал аутентификации, протокол Magparing, АП-коды.

1. Введение. Защита информации в беспроводных сетях по-прежнему является актуальной проблемой. Гарантированная защита,

как известно, достигается применением криптографических методов шифрования и аутентификации, для реализации которых нужны ключи. Многие мобильные устройства в сетях мобильной связи и Wi-Fi сетях содержат встроенные алгоритмы криптографической защиты, которые активируются оператором связи. Однако пользователи беспроводных сетей не всегда могут быть информированы об условиях подключения этих алгоритмов и уверены в их реализации. В связи с этим развиваются способы создания безопасного соединения между двумя абонентами без помощи доверенной третьей стороны. Например, одним из способов установления безопасного канала связи между двумя устройствами мобильной связи является технология защиты информации «Конфиденциальная сотовая связь» [1]. Данная технология предполагает приобретение пользователем специального телефона, например SMP-Атлас-2 или M-539, M-549. Недостаток использования этих телефонов заключается в их высокой стоимости и необходимости приобретать ключи у оператора.

Другой вариант решения этой задачи — переход к гибридной схеме, в которой распределение ключей осуществляется пользователями при помощи асимметричного алгоритма, а шифрование — при помощи симметричного алгоритма на парных ключах, созданных с и использованием технологий ассиметричных ключей. Каналы распределения открытых ключей должны быть аутентифицированы, что, в свою очередь, требует либо создания сети доверия по типу программы PGP [2], либо подключения к инфраструктуре открытых ключей (PKI) и использования сертификатов для аутентификации ключей. [3].

В последнее время получили широкое развитие технологии формирования ключа для мобильных устройств на основе использования случайных параметров каналов связи между ними, которые называются технологиями безопасности физического уровня (physical layer security) [4-6]. В [7-9] исследуются способы формирования ключа между мобильными корреспондентами на основе использования случайностей коэффициентов передачи MIMO (MISO) каналов. В [10, 11] проведено исследование и получены характеристики скорости формирования ключа в MIMO-канале на основе оценивания фазы принимаемого сигнала в предположении соблюдения принципа взаимности, то есть равенства передаточных матриц от корреспондента A к корреспонденту B и обратно. В [12-14] проведены исследования способа формирования ключа посредством MIMO-канала без использования принципа взаимности. Другие способы распределения ключей в рамках этого же направления исследований дополнительно привлекают третью доверенную сторону или ретрансляторы [15].

При таких способах распределения ключей важно, чтобы эти ключи были аутентифицированы, что, в свою очередь, требует либо предварительно разделенного секрета между парами пользователей или их аутентификации каким-либо другим способом.

В связи с этим представляется актуальным направление обеспечения ключами пользователей на основе реализации сценария сопряжения (спаривания) мобильных устройств (смартфонов, планшетов и пр.) при личной встрече пользователей и выполнения процедуры близкой аутентификации (near authentication) [16-18].

В настоящей работе исследуется способ аутентификации ключа, формируемого по методу Диффи — Хеллмана (DH), [19] между двумя пользователями с помощью создания кратковременного дополнительного канала обмена магнитометрическими данными при взаимном сближении мобильных устройств (смартфонов).

В первой части работы анализируются способы создания дополнительного канала обмена данными между пользователями для аутентификации ключа. Показано, что наилучшим является канал на основе измерений магнитного поля магнитометром в составе мобильного устройства. Во втором разделе приводится детальный анализ протокола аутентификации ключа на основе магнитометрических данных «MagParing» [20]. Показано, что данный протокол уязвим к атаке «человек посередине». В третьей части работы приведены результаты исследования протокола «MagParing» с помощью программы «AVISPA». В пятом разделе предлагается способ аутентификации ключа, распределяемого по методу Диффи — Хеллмана, на основе использования аутентифицирующих помехоустойчивых кодов. В шестом разделе разработан подход к оптимизации параметров АП-кодов для обеспечения заданных требований к длине формируемого ключа, вероятности ложного отклонения ключа, вероятности приема ложного ключа и минимальной длине аутентифицирующей последовательности. В заключении представлены итоги исследования.

Вклад настоящей работы в исследуемую проблему состоит в следующем:

1. Показана уязвимость протокола MagParing, использующего магнитометрические данные для аутентификации сторон при распределении ключей по методу Диффи — Хеллмана к атаке человек посередине.

2. Подтверждена уязвимость протокола MagParing с помощью программы AVISPA, используемой для анализа безопасности протоколов.

3. Разработан способ аутентификации сторон при распределении ключей по методу Диффи — Хеллмана на основе применения АП-кодов и магнитометрических данных.

4. Разработан подход к оптимизации параметров АП-кодов для обеспечения заданных требований: к длине формируемого по методу Диффи — Хеллмана ключа, вероятности ложного отклонения ключа, вероятности приема ложного ключа при минимальной длине аутентифицирующей последовательности.

2. Способы создания дополнительного канала для аутентификации сторон, использующих метод Диффи — Хеллмана **для распределения ключа между ними.** Рассмотрим двух пользователей сети, назовем их Алиса (*A*) и Боб (*B*), которые вырабатывают совместный ключ, используя метод Диффи — Хеллмана [19]. Пользователи *A* и *B*, согласуют общие параметры *p* и *g*, где *p* — просто число, а *g* — элемент конечного поля $GF(p)$, который порождает группу, имеющую большой порядок. Далее выполняется следующий протокол:

1. Алиса генерирует элемент $x \in (1, p-1)$, вычисляет $X = g^x \pmod p$ и посылает его Бобу.
2. Боб генерирует элемент $y \in (1, p-1)$, вычисляет $Y = g^y \pmod p$ и посылает его Алисе.
3. Алиса вычисляет ключ $K = Y^x \pmod p$.
4. Боб вычисляет ключ $K = X^y \pmod p$.

Легко увидеть, что ключи, найденные Алисой и Бобом, равны $K = g^{yx} \pmod p = g^{xy} \pmod p$.

Далее величины *X,Y,* которые передаются по открытым каналам, будем называть значениями Диффи — Хеллмана (DH).

Таким образом, метод Диффи — Хеллмана позволяет использовать незащищенный от перехвата канал связи для генерирования общего ключа шифрования с целью создания безопасного соединения между двумя корреспондентами. Однако пользователи не могут достоверно определить, кем является их собеседник, так как данный протокол чувствителен к атаке «человек посередине». Алиса и Боб могут оказаться в ситуации, при которой они установили связь с злоумышленником — Евой (E), которая Алисе выдает себя за Боба, а Бобу представляется Алисой. Поэтому для дальнейшей совместной работы Алисе и Бобу требуется аутентифицировать ключи, сгенерированные по методу Диффи — Хеллмана.

Эта задача может быть решена на основе использования дополнительных (Out-Of-Band — OOB) каналов: визуального, акустического, вибрационного, тактильного или магнитометрического [20-30]. Дополнительный канал образуется между двумя мобильными устрой-

ствами при личной встрече пользователей и не требует передачи какой-либо информации по каналу связи, затрудняя тем самым проведение атак со стороны злоумышленника.

Аутентификация по дополнительному каналу применима в тех случаях, когда пользователи имеют непосредственный доступ к устройствам, которые должны аутентифицировать друг друга. После проведения взаимной аутентификации устройства могут устанавливать защищенное соединение и обмениваться данными, используя сформированный по методу Диффи — Хеллмана ключ.

Для краткости будем называть обмен данными по дополнительному каналу с целью аутентификации сторон *сопряжением мобильных устройств*.

Поскольку участие пользователей при аутентификации по дополнительному каналу неизбежно, решающими факторами являются удобство использования и защита передаваемых данных. Кроме того, поскольку канал OOB обладает низкой пропускной способностью, объем информации, передаваемой по нему, должен быть сведен к минимуму. Проведем анализ дополнительных каналов связи.

Визуальный канал. Один из способов этой группы, получивший название «Seeing-is-Believing» (SiB) [21] предполагает, что устройство *A* формирует двухмерный штрих-код, который является графическим аналогом хэш-функции ключевой информации, переданной ранее устройству *B*. Устройство *B* для проверки подлинности ключа считывает штрих-код при помощи фотокамеры и сравнивает значение хэш-функции со значением хэш-функции, вычисленной из полученной ключевой информации. В случае совпадения хэш-кодов ключ считается подлинным.

Недостаток способа в том, что взаимная аутентификация выполняется в виде двух отдельных однонаправленных шагов аутентификации. Поэтому для ускорения аутентификации предложен метод Visual authentication based on Integrity Checking (VIC) [22]. VIC представляет собой способ, в котором каждому устройству требуется вычислить общую хэш-функцию от публичных данных (ключей) и сравнить полученные результаты, используя визуальный OOB канал.

Поскольку для реализации VIC нужен только один однонаправленный визуальный OOB канал, устройство одного из пользователей может не иметь камеры.

Для устройств, не имеющих экранов и камер, предложен способ, который основан на «мигании» светодиода и получил название «Blink-Blink» [23]. LED-устройство для подтверждения подлинности передает ключевую информацию на приемник, оснащенный датчиком обнаружения света или видеокамерой. Принимающая сторона декоди-

рует полученное сообщение, основываясь на длительности каждого не подающего свет интервала (долгое прерывание света представляет собой «1», короткое — «0») и сравнивает полученные по визуальному каналу данные со своими данными.

Акустический канал. Аутентификация устройств с использованием *акустического канала* связи предполагает передачу звукового сигнала от динамика, расположенного на стороне источника, до микрофона, находящегося на приемной стороне.

Способ Beep-Beep [24] в акустическом OOB канале является альтернативой Blink-Blink и имеет тот же принцип работы, что и его визуальный прототип. Сопряжение устройств основано на работе звукового динамика, передающего информацию при помощи прерывистого звукового сигнала на стороне источника и микрофона на стороне приемника. Принимающая сторона декодирует полученное сообщение (длинный гудок представляет собой «1», короткий — «0») и сравнивает полученные по акустическому каналу данные со своими.

Способ Loud-and-Clear (L&C) [25] позволят преобразовывать символьную строку в голосовой поток. Система L&C в работе использует библиотеку Madlib, содержащую список всех возможных для передачи символов и соответствующие каждому символу слова. Способ L&C предполагает, что для аутентификации устройство *A* вычисляет хэш-функцию переданной ранее ключевой информации, преобразует ее значение в последовательность слов, основываясь на библиотеке Madlib, и передает полученное предложение устройству *B*. Устройство *B* декодирует сообщение и сравнивает его со значением хэш-функции, вычисленной из полученной ранее от пользователя *A* ключевой информации. Способ L&C предполагает, что хотя бы одно из двух устройств должно иметь звуковой динамик, тогда как другое устройство должно иметь микрофон и/или дисплей. Аутентификации по методу L&C требует длительного времени для того, чтобы пользователь мог сравнить два голосовых потока или один голосовой поток с последовательностью слов, представленных в текстовом виде.

Альтернативой L&C является метод Human-Assisted Pure Audio Device Pairing (HAPADEP), использующий для аутентификации пользователей только динамик и микрофон [26]. Проверка подлинности устройств по методу HAPADEP базируется на преобразовании ключевой информации в короткую мелодию, которую можно сыграть на фортепиано.

Все методы аутентификации по акустическому каналу подвержены влиянию акустического шума в месте приема.

Вибрационный канал. Использование для аутентификации мобильных устройств дополнительного вибрационного канала

представляется возможным для устройств, содержащих в себе датчики акселерометра, позволяющие считать информацию о положении мобильного устройства в пространстве и преобразовать ее в цифровой код.

В способе Smart-Its Friends [27] предполагается, что для генерирования общего ключа два мобильных устройства необходимо встряхивать, удерживая их в одной руке. При этом считывается информация от датчика акселерометра о положении мобильного устройства в пространстве, которая далее преобразуется в цифровой код.

Два устройства (*A* и *B*), которые трясли вместе, на выходе получат схожие ключевые последовательности. В данном способе ключевые данные, формируемые непосредственно между пользователями, могут в точности не совпадать. Для их согласования требуется отдельный канал передачи и, соответственно, аутентификация в нем.

Поэтому более практичным является способ Shaking for Verification (ShaVe) [28], в котором ключ шифрования, формируется по методу Диффи — Хеллмана, а для аутентификации ключа в устройствах формируются идентичные случайные последовательности на основе показаний датчиков акселерометров во время совместного встряхивания сопрягаемых устройств.

Тактильный канал. Основывается на нажатии пользователем кнопок на мобильных устройствах.

Button-Enabled Device Association (BEDA) — набор протоколов безопасного сопряжения устройств, в состав которого входят протоколы LED-Button, Beep-Button, Vibration-Button и Button-Button [29]. Работа данных протоколов предполагает, что одно (или даже оба) устройства имеют только одну кнопку в качестве «пользовательского интерфейса». Вспомогательный канал, включенный одной кнопкой, служит основой для обеспечения безопасности основного канала связи, такого как Bluetooth или Wi-Fi.

В первых двух вариантах передающее устройство сигнализирует вспышками LED, вибрацией или звуками микрофона. Пользователь, наблюдая эти сигналы, должен нажать кнопку на приемном устройстве. Предполагается, что сигналы передающей стороны не подлежат перехвату.

В способе Button-Button пользователь одновременно нажимает кнопки на обоих устройствах, а случайные пользовательские задержки нажатия кнопок используются в качестве средства установления общего секрета.

Магнитометрический канал. Способ аутентификации на основе использования данных магнитометров, входящих в состав мобильных устройств, предложен в [20], и получил название MagPairing.

Согласно MagPairing, пользователям необходимо удерживать два устройства вблизи друг к другу несколько секунд без выполнения каких-либо дополнительных операций. Устройства считывают собственные показания датчиков магнитометра и обмениваются ими. Из этих данных формируется последовательности, на основе которых осуществляется аутентификация распределенного по методу DH ключа.

Сравнительная характеристика рассмотренных выше способов аутентификации мобильных устройств, выполненная на основе работ [20, 30], приведена в таблице 1.

Таблица 1. Сравнительная характеристика дополнительных каналов аутентификации ключа

Вид дополнит. канала	Способ аутентификации	Требования к устройствам		Время сопряжения	Вероятность ошибки
		устройство А	устройство В		
Визуальный	SiB	Дисплей+Камера	Дисплей+Камера	26.9 с	5%
	VIC	Дисплей+Камера	Дисплей+Камера, Камера или дисплей	17.0 с	5%
	Blink-Blink	Дисплей+Камера	Дисплей+Камера, Камера или дисплей	24.9 с	5%
Акустический	Beep-Beep	Динамик+Микрофон	Динамик+Микрофон, Камера или микрофон	25.0 с	20%
	Loud-and-Clear	Динамик+Микрофон	Динамик+Микрофон	15.5 с	10%
	HAPADEP	Динамик+Микрофон	Динамик+Микрофон, Динамик или микрофон	10.8 с	5%
Вибрационный	PIN-Vibra	Акселерометр	Микрофон	9.5 с	20%
	Smart-Its Friends	Акселерометр	Акселерометр	10.4 с	10%
	ShaVe	Акселерометр	Акселерометр	10.8 с	5%
	ShaCK	Акселерометр	Акселерометр	14.0 с	10%
Тактильный	LED-Button	Дисплей	Камера+Кнопка	27.5 с	5%
	Beep-Button	Динамик	Микрофон+Кнопка	16.8 с	5%
	Vibration-Button	Акселерометр	Микрофон+Кнопка	18.0 с	5%
	Button-Button	Кнопка	Кнопка	32.1 с	5%
Магнитометрический	MagPairing	Магнитометр	Магнитометр	4.5 с	7%

Каждый способ оценивался по трем характеристикам: требования к сопрягаемым устройствам, время, необходимое для их сопряжения, и вероятность ошибочной аутентификации устройств.

Видим, что способы, основанные на визуальном канале, имеют наименьшую вероятность ошибки, хотя требуется большое время для аутентификации. Способы, основанные на акустическом канале, имеют большую вероятность ошибки и требуют большего времени. Применение вибрационного канала для реализации процесса аутентификации требует наличия у мобильных устройств датчиков акселерометра и встряхивания мобильных устройств пользователем в течение примерно 5 с. Показатели по времени аутентификации и вероятности ошибки — средние. Аутентификация по тактильно каналу занимает достаточно много времени, хотя и имеет невысокую вероятность ошибки, а также требует наличия кнопки для инициирования начала/конца процедуры аутентификации.

Сопряжение с использование м магнитометрического канала связи обеспечивает высокую скорость работы (4,5 секунды), низкую вероятность ошибочной аутентификации и позволяет минимизировать участие пользователя в процессе сопряжения устройств, что указывает на преимущество использования магнитометрического канала связи для аутентификации мобильных устройств. Поэтому далее в работе рассматривается аутентификация не основе магнитометрических данных, вырабатываемых мобильными устройствами при их сопряжении.

3. Анализ уязвимостей протокола Magpairing. Формирование ключа по методу Диффи — Хеллана с использованием протокола аутентификации MagPairing [20] включает четыре этапа (рисунок 1).

1-й этап. Пользователи A и B проводят процедуру сопряжения мобильных устройств (смартфонов). Для этого они располагают устройства достаточно близко друг к другу (касаются друг друга) и удерживают несколько секунд. В это время в каждом смартфоне производится измерение магнитного поля по трем пространственным осям X, Y, Z. Значения магнитного поля квантуются и из них формируются двоичные последовательности, которые позже используются для аутентификации ключа, распределяемого по методу Диффи — Хеллмана.

Далее осуществляется локальный обмен данными, например, по каналу Bluetooth, для коррекции последовательностей с целью обеспечения их идентичности. В итоге каждое устройство формирует случайную двоичную последовательность необходимой длины. Обозначим последовательности пользователей A и B, как M_A и M_B соответственно. В [20] подробно описан процесс сбора и коррекции данных магнитометров. Мы не будем описывать эти результаты, поскольку они составляют предмет отдельного исследования, отметим лишь, что нами были проведены аналогичные исследования [31], которые подтвердили результаты работы [20]. Вероятность совпадения бит двух последовательностей от разных устройств в наших экспериментах составила 0.94.

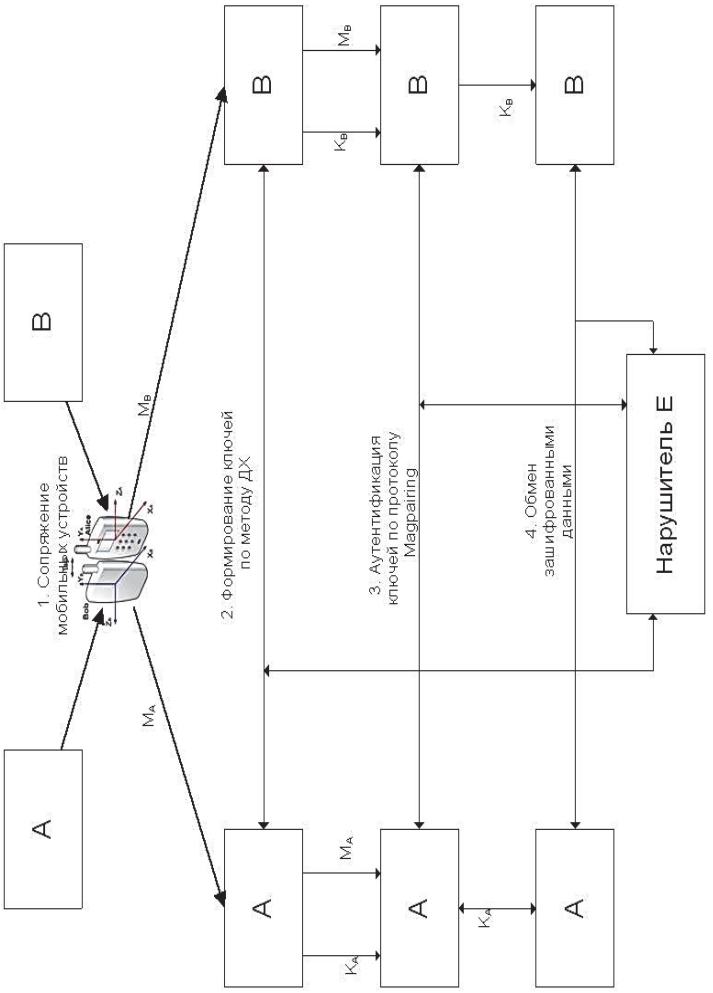

Рис.1. Сценарий формирования и аутентификации ключа

Предполагается, что нарушитель также имеет магнитометр и на этом этапе может быть расположен достаточно близко к сопрягаемым устройствам, но не в точке сопряжения, что определяется организационными ограничениями. Перехват данных коррекции нарушителем возможен, но это не приводит к утечке данных магнитометра.

2 этап. Пользователи вырабатывают секретный ключ по методу Диффи — Хэллмана, используя для этого канал связи между ними. Канал связи может контролироваться нарушителем. Он может выполнять пассивные и активные атаки на передаваемую информацию.

3-й этап. С целью защиты от атак нарушителя проводится аутентификация переданных по каналу связи данных (ключей) на основе полученных на первом этапе последовательностей M_A и M_B, с использованием протокола MagPairing.

4-й этап. Если аутентификации прошла успешно, ключи, сформированные по методу DH, используются для шифрования информации, передаваемой между пользователями.

Обозначим: K — ключ, сформированный по методу DH. $\boldsymbol{a}$ — случайная последовательность у корреспондента A, полученная путем конкатенации M_A и идентификатора (ID_A), $\boldsymbol{b}$ — случайная последовательность у корреспондента B, полученная путем конкатенации M_B и идентификатора (ID_B). Будем также использовать обозначение: $c[x, y]$ — строка бит $\boldsymbol{c}$, начинающаяся битом с номером x и заканчивающаяся битом с номером y.

Проведем анализ протокола аутентификации ключей MagPairing [20] (рисунок 2).

1. Корреспонденты A и B, формируют сессионные ключи K_A и K_B по методу Диффи — Хеллмана.

2. Корреспонденты A, B генерируют строки $\boldsymbol{a}$ и $\boldsymbol{b}$, в которых показания датчиков магнитометра M_A и M_B конкатенируются с идентификаторами самих устройств.

3. Корреспонденты A, B генерируют случайные стартовые векторы: $\boldsymbol{c}_0$, $\boldsymbol{d}_0$.

4. Строки данных $\boldsymbol{a}$ и $\boldsymbol{b}$, суммируются со стартовыми векторами. Результат суммирования шифруется по алгоритму AES в режиме CBC на ключах K_A и K_B соответственно. Формируются криптограммы: $\boldsymbol{c} = E(K, \boldsymbol{c}_0 \oplus \boldsymbol{a})$, $\boldsymbol{d} = E(K, \boldsymbol{d}_0 \oplus \boldsymbol{b})$.

5. Корреспондент A посылает корреспонденту B строку $A1$, состоящую из половины своего нешифрованного стартового вектора $\boldsymbol{c}_0$ и половины криптограммы $\boldsymbol{c}$: $A1 = \boldsymbol{c}_0[0,63] \| \boldsymbol{c}[0,63]$.

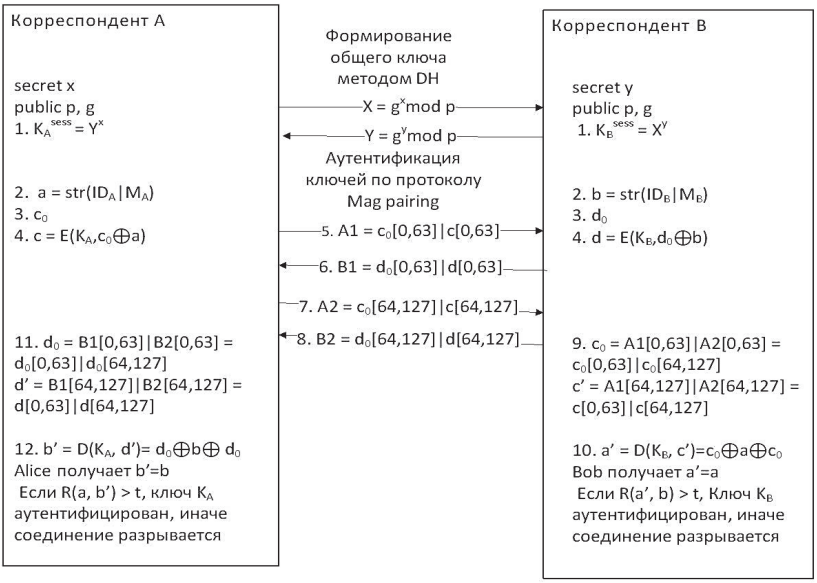

Рис. 2. Аутентификация ключей по протоколу MagPairing

6. Корреспондент *B*, не имеющий возможности дешифровать полученную строку, отправляет корреспонденту *A* строку *B1* со своими значениями, построенными по тому же принципу, что и *A1*: $B1 = \boldsymbol{d_0}[0,63] \| \boldsymbol{d}[0,63]$.

7. Корреспондент *A* также не может дешифровать данное сообщение. *A* отправляет *B* строку *A2*, состоящую из второй половины своего стартового вектора $\boldsymbol{c_0}$ и второй половины криптограммы $\boldsymbol{c}$: $A2 = \boldsymbol{c_0}[64,128] \| \boldsymbol{c}[64,128]$.

8. После получения *A2*, корреспондент *B* посылает *A* сообщение, состоящее из вторых частей последовательностей $\boldsymbol{d_0}$ и $\boldsymbol{d}$: $B2 = \boldsymbol{d_0}[64,128] \| \boldsymbol{d}[64,128]$.

9. Корреспондент *B* восстанавливает сообщения $\boldsymbol{c_0}$ и $\boldsymbol{c'}$, объединяя первые и вторые части *A1* и *A2* соответственно:
$\boldsymbol{c_0} = A1[0,63] | A2[0,63] = \boldsymbol{c_0}[0,63] | \boldsymbol{c_0}[64,127]$,
$\boldsymbol{c'} = A1[64,127] | A2[64,127] = \boldsymbol{c}[0,63] | \boldsymbol{c}[64,127]$.

10. Корреспондент B, дешифрует $\boldsymbol{c'}$, получает строку $\boldsymbol{a'=a}$ и вычисляет коэффициент корреляции $R(a',b)$ между последовательно-

стью $\boldsymbol{a'}$, полученной от A, и последовательностью $\boldsymbol{b}$, сформированной самим устройством B, по формуле $R = 1 - \frac{2}{l} D(\boldsymbol{a'},\boldsymbol{b})$, где D — расстояние Хэмминга между последовательностями $\boldsymbol{a'}$ и $\boldsymbol{b}$ длины l. Если коэффициент $R(\boldsymbol{a'},\boldsymbol{b}) \geq t$, где t заранее установленный порог, корреспондент B подтверждает подлинность A, иначе соединение прерывается.

11. Корреспондент A восстанавливает строки $\boldsymbol{d_0}$ и $\boldsymbol{d'}$, объединяя первые и вторые части $B1$ и $B2$ соответственно.

12. Корреспондент A дешифрует $\boldsymbol{d'}$ и сравнивает полученное значение $\boldsymbol{b'}$ показаний датчика со своим значением $\boldsymbol{a}$.

Если коэффициент корреляции $R(\boldsymbol{a'},\boldsymbol{b}) \geq t$, то сгенерированный по методу Диффи — Хеллмана ключ аутентифицируется как подлинный, иначе соединение прерывается.

В [20] проведен анализ протокола к следующим атакам: пассивная атака, атака отражения, атака с повторной передачей и атака человек посередине.

Пассивная атака. При пассивной атаке нарушитель не прерывает процесс согласования ключей, следит за протоколом MagPairing. Легальные пользователи могут успешно сгенерировать и аутентифицировать ключ Диффи — Хеллмана, устойчивый к данной атаке, поскольку его криптостойкость основана на высокой вычислительной сложности решения задачи дискретного логарифмирования.

Атака отражением. Злоумышленник может перехватывать и пересылать обратно сообщения, отправленные Алисой и Бобом. В результате Алиса и Боб получат свои собственные данные датчиков, дающие высокий уровень корреляции, и как бы аутентифицируют друг друга. Однако эта атака может быть легко обнаружена проверкой идентификатора (ID) отправителя сообщения.

Атака с повторной передачей. Атакующий может сохранить показания датчиков магнитометров, переданные в первой сессии, и воспользоваться ими при второй попытке сопряжения устройств. Однако эта атака не будет успешной, так как данные магнитных датчиков второй сессии в силу случайности будут отличаться от данных первой сессии, а коэффициент корреляции будет низким.

Атака «человек посредине». Атака «человек посередине» основана на подмене одного пользователя другим. Нарушитель, выступая от имени одной из сторон и полностью имитируя ее действия, получает в ответ сообщения определенного формата, необходимые для подделки отдельных шагов протокола. Атака достигается атакующим, который создает независимые ключи K_A, K_B по методу Диффи —

Хеллмана с каждым корреспондентом. При этом корреспонденты полагают, что они «разговаривают» напрямую друг с другом, но на самом деле весь разговор контролируется атакующим.

Стойкость протокола MagPairing к атаке «человек посередине», по мнению авторов [20], основана на том, что сообщения $\boldsymbol{c_0}$ и $\boldsymbol{c}$ передаются не сразу, а равными частями. Половина зашифрованного сообщения не может быть расшифрована пока не будет получена вторая половина этого сообщения. А вторая половина не будет отправлена пока инициатор установления соединения не получит первую половину сообщений от ответчика $\boldsymbol{d_0}$ и $\boldsymbol{d}$.

Рассмотрим теперь вариант выполнения протокола аутентификации MagPairing, предполагая, что нарушитель проводит дополнительно атаку *перехват-пересылка* на этапе процедуры аутентификации ключа. Инициатором процедуры аутентификации выступает один из корреспондентов, например *A*. На первом этапе *A* и *E* обмениваются первыми половинами сообщений, далее *A* отправляет *E* вторую половину своего сообщения, что позволяет устройству *E* узнать значения данных датчиков магнитометра *A* и зашифровать их на ключе сгенерированном совместно с *B* (рисунок 3). Рассмотрим более детально эту атаку.

1. Корреспонденты *A* и *B*, подверженные атаке «человек посередине», формируют секретные ключи совместно с нарушителем *E* по алгоритму Диффи — Хеллмана.

2. Корреспонденты *A, B* и *E* генерируют строки $\boldsymbol{a, b, e}$, в которых показания датчиков магнитометра конкатенируются с идентификаторами самих устройств.

3. Корреспонденты *A, B* и *E* генерируют случайные стартовые векторы $\boldsymbol{(c_0, d_0, f_0, h_0)}$.

4. Строки данных, полученные после конкатенации, суммируются со стартовыми векторами. Результаты суммирования шифруются по алгоритму AES на ключах Диффи — Хеллмана $\boldsymbol{c=E(K_A, c_0 \oplus a)}$, $\boldsymbol{f=E(K_{AE}, f_0 \oplus e_1)}$, $\boldsymbol{h=E(K_{EB}, h_0 \oplus e_2)}$, $\boldsymbol{d=E(K_B, d_0 \oplus b)}$.

5. Корреспондент *A* посылает *E* строку *A1*, состоящую из половины своего стартового вектора $\boldsymbol{c_0}$ и половины криптограммы $\boldsymbol{c}$: $A1 = \boldsymbol{c_0}[0,63] \| c[0,63]$.

6. Злоумышленник *E*, не имеющий возможности дешифровать полученную строку, отправляет корреспонденту *A* строку $E_A1 = \boldsymbol{f_0}[0,63] \| \boldsymbol{f}[0,63]$ со своими значениями, построенными по тому же принципу, что и *A1*.

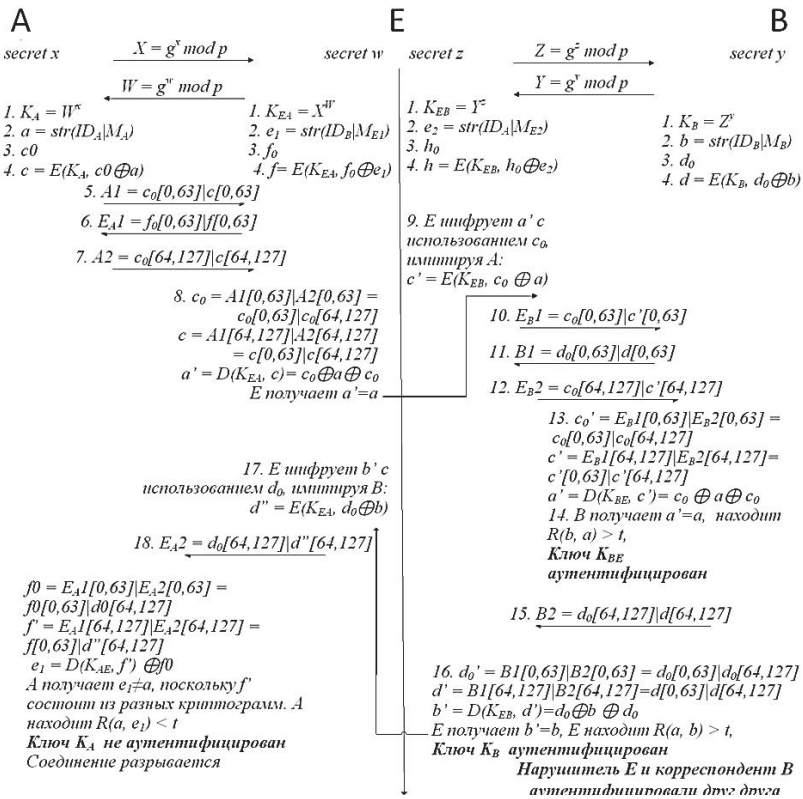

Рис. 3. Протокол MagPairing в условиях активного перехвата

7. Корреспондент *A* также не может дешифровать данное сообщение. *A* отправляет *E* строку *A2*, состоящую из второй половины своего стартового вектора $\boldsymbol{c_0}$ и второй половины криптограммы $\boldsymbol{c}$: $A2 = \boldsymbol{c_0}[64,128]|\boldsymbol{c}[64,128]$.

Аналогичные операции проводят корреспондент *B* и злоумышленник *E*.

Нарушителю *E* дальше нет смысла повторять действия корреспондентов *A* и *B* (п.8 протокола MP), так как это приведет к обнаружению атаки, поскольку априори строки $\boldsymbol{a,e_1}$ и $\boldsymbol{b,e_2}$ разные. Поэтому он далее развивает атаку перехват-пересылка на основе данных, полученных от *A* и *B*.

8. Из сообщений *A1* и *A2* нарушитель восстанавливает строки $\boldsymbol{c0}$ и $\boldsymbol{c}$, расшифровывает $\boldsymbol{c}$, получает строку бит $\boldsymbol{a}$ и продолжает протокол аутентификации под видом корреспондента *A*.

9. Нарушитель E на основе полученных строк $\boldsymbol{a}$ и $\boldsymbol{c_0}$ формирует строку $\boldsymbol{c'=E(K_{EB}, c_0 \oplus a)}$ с использованием ключа K_{EB}, сгенерированного совместно с устройством B.

10. Нарушитель E, отправляет корреспонденту B сообщение: $E_B 1 = \boldsymbol{c_0}[0,63] \,|\, \boldsymbol{c'}[0,63]$, состоящее из первых частей блоков $\boldsymbol{c_0}$ и $\boldsymbol{c'}$.

11. Корреспондент B, не имея пока возможности дешифровать полученную строку, отправляет E строку $B1 = \boldsymbol{d_0}[0,63] \,|\, \boldsymbol{d}[0,63]$, построенную по тому же принципу, что и строка $A1$.

12. Нарушитель E отправляет B строку $E_B 2$, состоящую из второй половины стартового вектора A и второй половины блока $\boldsymbol{c'}$: $E_B 1 = \boldsymbol{c_0}[64,127] \,|\, \boldsymbol{c'}[64,127]$.

13. Корреспондент B восстанавливает блоки $\boldsymbol{c_0}$ и $\boldsymbol{c'}$, дешифрует $\boldsymbol{c'}$ и вычисляет показания датчика магнитометра $\boldsymbol{a'}$ корреспондента A.

14. Корреспондент B находит коэффициент корреляции $R(\boldsymbol{b,a'})$. Так как нарушитель, обмениваясь сообщениями с корреспондентом B, ретранслировал фактические значения показаний датчика магнитометра A, то с большой вероятностью $R(\boldsymbol{b,a'}) \geq t$. Таким образом, B подтверждает подлинность корреспондента A. Но на самом деле он установил соединение с нарушителем E.

15. Корреспондент B отправляет E ответное сообщение: $B2 = \boldsymbol{d_0}[64,127] \,|\, \boldsymbol{d}[64,127]$.

16. Нарушитель E на основе сообщений $B1$ и $B2$ формирует строки $\boldsymbol{d'}$ и $\boldsymbol{d_0}$. Дешифрует $\boldsymbol{d'}$ с использованием ключа K_{EB}, сгенерированного совместно с корреспондентом B. Находит коэффициент корреляции $R(\boldsymbol{a',b})$. Если магнитометрические данные A и B отличаются не сильно, то с большой вероятностью $R(\boldsymbol{a',b}) \geq t$. В результате E аутентифицировал корреспондента B, хотя последний считает, что он работает с A.

17. Нарушитель E, получив необходимые данные от устройства B, шифрует $\boldsymbol{b}$ с использованием $\boldsymbol{d_0}$.

18. E отправляет корреспонденту A сообщение: $E_A 2 = \boldsymbol{d_0}[64,127] \,|\, \boldsymbol{d'}[64,127]$.

19. Корреспондент A восстанавливает блоки $\boldsymbol{f_0}$ и $\boldsymbol{f'}$, дешифрует $\boldsymbol{f'}$ и вычисляет показания датчика магнитометра $\boldsymbol{e}'_1$ нарушителя E, предполагая, что это B. A сравнивает данные, полученные от E, со своими данными. Так как нарушитель, использовал ложные значения по-

казаний датчика магнитометра $\boldsymbol{e}_1$, то вычисленный A коэффициент корреляции $R(\boldsymbol{a}, \boldsymbol{e}1') < t$. Соединение между A и E прерывается.

Анализ протокола показывает, что используя атаку «человек посередине», нарушитель может сформировать ключи с каждым из корреспондентов и, пройдя аутентификацию по протоколу MagPairing, *установить соединение с одним из корреспондентов, выдав себя за второго.* Это позволяет сделать вывод о недостаточной стойкости протокола MagPairing для аутентификации ключей, распределяемых по методу Диффи—Хэллмана. В связи с этим является актуальной разработка протокола, устойчивого к подобного рода атакам нарушителя.

4. Анализ уязвимости протокола аутентификации ключей MagPairing с использованием программы AVISPA. Важным этапом анализа защищенных протоколов передачи данных является стадия оценки их безопасности, на которой проверяется стойкость протоколов к различным видам атак. Известно большое число различных подходов к анализу уязвимости протоколов. Одним из них является использование программы AVISPA (Automated Validation of Internet Security Protocols and Applications), позволяющей не только находить уязвимости у того или иного протокола, но и определять возможные атаки на него [32].

Архитектура AVISPA допускает анализ протокола одним из четырех модулей: «OFMC», «CL-AtSe», «SATMC», «TA4SP»

Каждый из модулей представляет собой уникальный верификатор, который может использоваться как самостоятельно, так и в сочетании с другими модулями. Модуль OFMC (On-the-Fly Model-Checker) является анализатором для проверки протокола методом «инертного злоумышленника» и используется в случаях, когда сообщения злоумышленника представлены выражениями с переменными, значения которых не фиксируются. Модуль CL-AtSe (constraint-Logic-based Model-Searcher) — программа верификации, основанная на логике ограничений, которые обязывают нарушителя выполнять определенные действия. Эти действия могут быть эффективно использованы для нахождения атак на протоколы. Модуль SATMC (SAT-based Model-Checker) основан на методах теории решения задач планирования. А модуль TA4SP (Tree Automata based on Automatic Approximations for the Analysis of Security Protocols) является инструментом доказательства свойств безопасности протоколов и позволяет производить доказательства при неограниченном числе сессий на основе знаний нарушителя.

Спецификация анализируемого протокола, основанная на ролевом представлении, записывается на языке высокого уровня HLPSL (High Level Protocol Specification Language), который затем переводится в более низкоуровневый язык IF, что позволяет более де-

тально описывать протоколы по сравнению с аналогами. Результаты, полученные с помощью AVISPA, подробны и конструктивны.

С помощью программы AVISPA была спроектирована модель проверки протокола MagPairing в условиях активного перехвата [33].

На листинге 1 представлено описание протокола на языке HLPSL:

```
// Начало протокола
        role role_A(A:agent,
B:agent,C01:text,C02:text,C1:text;C2:text,SND,RCV:channel(dy))
        played_by A
        def=
                local
                        State:nat,D01:text,D1:text,D02:text;D2:text
                init
                                State:=0
                transition
                                1.State=0/\RCV(start)=|>State':=1/\SND(C01.C1)
                                2.State=1/\RCV(D01'.D1')=|>State':=2/\SND(C02.C2)
                                3.State=2/\RCV(D02'.D2')=|>State':=3
        end role
        role role_B(A:agent,
B:agent,D01:text,D02:text,D1:text;D2:text,SND,RCV:channel(dy))
        played_by AB
        def=
                local
                        State:nat,C01:text,C1:text,C02:text;C2:text
                init
                                State:=0
                transition
                                1.State=0/\RCV(C01'.C1')=|>State':=1/\SND(D01.D1)
                                2.State=1/\RCV(C01'.C1')=|>State':=2/\SND(D02.D2)
        end role
        role session(C01:text,C02:text,C1:text;C2:text, A:agent,
B:agent,D01:text,D02:text,D1:text;D2:text)
        def=
                local
                        SND2,RCV2,SND1,RCV1:channel(dy)
                composition
              role_B(A,B,D01,D02,D1;D2,SND2,RCV2)/\role_A(A,B,C01,C02,C1;C2,SND1,
RCV1)
        end role
        role environment()
        def=
                const
```

```
                hash_0:hash_func,d01:text,d02:text,alice:agent,c1:text,c2:text,c01:text,c02:te
xt,bob:
        agent,d1:text,d2:text,aec_1:protocol_id
                  intruder_knowledge={alice,bob,e01,e1}
                  composition
                session1(c2,c02,c1,c01,alice,bob,d01,d1,d02,d2)
         end role
         goal
                secrecy_of sec_1
         end goal
         environment()
// Конец протокола
```

Листинг 1. Описание протокола на языке HLPSL.

При компиляции кода, можно получить диаграмму передачи сообщений, которая наглядно описывает работу протокола MagPairing. Затем, после запуска модуля верификации OFMC, в окне программы появляется диаграмма передачи сообщений при участии злоумышленника (рисунок 4). В верхнем левом углу в поле «Incoming events» пользователю программы предложен список возможных для передачи между корреспондентами сообщений. Для установления алгоритма обмена данными необходимо переместить выбранное для передачи сообщение в поле «Past events», после чего на схеме появится изображение, указывающее направление передачи данного сообщения и его содержание. В нижнем левом углу представлены знания злоумышленника, которые он имел до начала сеанса передачи сообщения и после полного его завершения.

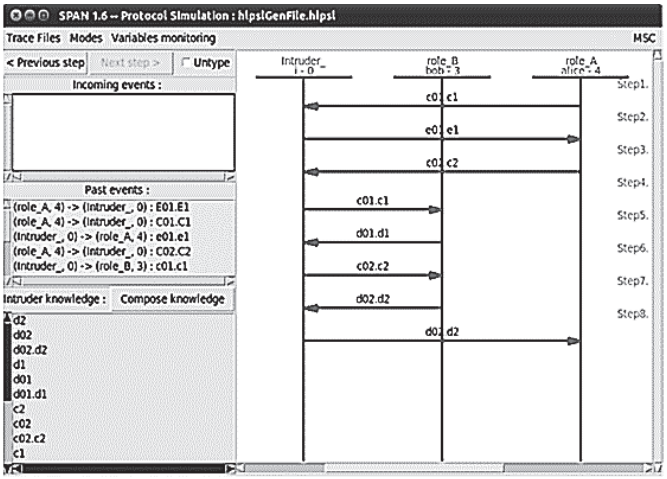

Рис. 4. Анализ MagPairing в программе AVISPA

В ходе анализа протокола MagPairing был определен порядок передачи сообщений, целью которого являлось получение злоумышленником данных одного легального корреспондента и передача их другому. Анализ показал, что, используя атаку «человек посередине», нарушитель может установить соединение с одним из корреспондентов, выдав себя за другого.

В итоге, с помощью программы AVISPA доказана уязвимость протокола MagPairing к атаке «человек посередине», что позволяет сделать вывод о недостаточной стойкости данного протокола аутентификации ключей.

5. Способ аутентификации ключей для метода Диффи — Хеллмана на основе магнитометрических данных и аутентифицирующих помехоустойчивых кодов. Как было показано выше, аутентификация ключей для метода DH, согласно протоколу MagPairing, не является безопасной. В этой связи предлагается для целей аутентификации использовать аутентифицирующие помехоустойчивые коды. Эти коды были впервые предложены в [34] и подробно исследованы в [35].

Дадим краткое описание способа построения таких кодов.

Предположим, что два корреспондента A и B связаны каналом связи без ошибок и имеют предварительно сформированные двоичные последовательности $\boldsymbol{a}$ и $\boldsymbol{b}$ соответственно. Вероятность несовпадения символов в этих последовательностях обозначим как $p_m = p(a_i \neq b_i)$, $i = 1, 2, ...$

Для построения АП-кода корреспонденты A и B заранее договариваются об использовании некоторого (n_a, k_a) — помехоустойчивого систематического кода V и о порядке сопоставления каждому сообщению $\boldsymbol{m}_i$ кодового слова $\boldsymbol{v}_i \in V$.

Если корреспондент A намерен передать сообщение $\boldsymbol{m}_i$ корреспонденту B, он выбирает кодовое слово $\boldsymbol{v}_i = (v_{i1}, v_{i2}, \ldots, v_{in_a})$ кода $\boldsymbol{V}$, $v_{ij} \in (0,1)$ и формирует аутентификатор $\boldsymbol{u}_i = (u_{i1}, u_{i2}, \ldots, u_{i\tau})$, используя имеющуюся у него аутентифицирующую последовательность $\boldsymbol{a}$ следующим образом. Для всех $j < n_a$, $u_{ij} = a_j$ если $v_{ij} = 1$, в противном случае u_{ij} не формируется. Далее сообщение $\boldsymbol{m}_i$ и аутентификатор $\boldsymbol{u}_i$ передаются по открытому каналу корреспонденту B. Очевидно, что длина τ аутентификатора $\boldsymbol{u}_i$ равна весу кодового слова $\boldsymbol{v}_i$.

Корреспондент B, приняв $(\boldsymbol{m}_i, \boldsymbol{u}_i)$, формирует $\boldsymbol{u}_i'$, используя для этого принятое сообщение $\boldsymbol{m}_i$ и аутентифицирующую последовательность $\boldsymbol{b}$ аналогично тому, как это делал корреспондент A. Далее он вы-

полняет сравнение аутентификаторов $\boldsymbol{u}_i$ и $\boldsymbol{u}_i'$ Если число совпадений в $\boldsymbol{u}_i$ и $\boldsymbol{u}_i'$ равно или больше некоторого порога Δ, то сообщение $\boldsymbol{m}_i$ считается подлинным, если меньше, сообщение $\boldsymbol{m}_i$ отвергается как ложное.

Рассмотрим далее способ применения АП-кода для аутентификации значений Диффи — Хеллмана на основе последовательностей $\boldsymbol{a}$ и $\boldsymbol{b}$, полученных от магнитометров мобильных устройств на этапе сопряжения устройств корреспондентами A и B [36]. Будем также называть последовательности $\boldsymbol{a}$ и $\boldsymbol{b}$ — *аутентифицирующими последовательностями*.

Рассмотрим следующий протокол аутентификации (рисунок 5).

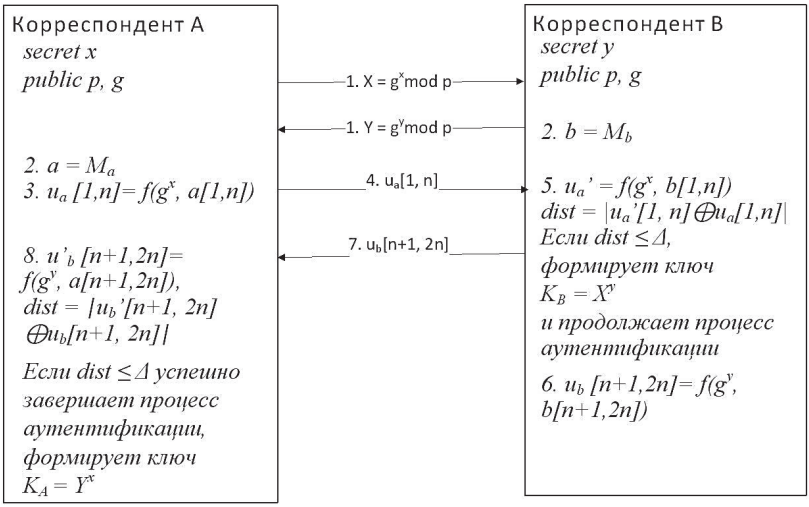

Рис. 5. Протокол аутентификации ключей на основе аутентифицирующих помехоустойчивых кодов с использованием магнитометрических данных

1. Корреспонденты A и B формируют значения DH: $X = g^x mod p$ и $Y = g^y mod p$ и обмениваются ими по каналу связи.

2. Корреспонденты A, B, используя магнитометрические данные — последовательности M_a и M_b, генерируют строки $\boldsymbol{a}$ и $\boldsymbol{b}$ длиной $2n$ бит.

3. Используя первые n бит последовательности $\boldsymbol{a}$, корреспондент A формирует аутентификатор $\boldsymbol{u}_a$ длиной n бит для последовательности $X = g^x mod p$ на основе АП-кода с параметрами $(2n, k, d)$.

4. Аутентификатор $\boldsymbol{u}_a$ передается корреспонденту *B*.

5. Корреспондент *B*, получив $X = g^x mod p$ и используя первые *n* бит своей последовательности $\boldsymbol{b}$, формирует местный аутентификатор $\boldsymbol{u}'_a$ и сравнивает его с аутентификатором $\boldsymbol{u}_a$, полученным от корреспондента *A*. Если число несовпадений символов для пары аутентификаторов $dist = \left| \boldsymbol{u}_a \oplus \boldsymbol{u}'_a \right|$ меньше некоторого порога Δ, значение *X* признается подлинным.

6. Используя вторые *n* бит последовательности $\boldsymbol{b}$, корреспондент *B* формирует аутентификатор $\boldsymbol{u}_b$ длиной *n* бит для последовательности $Y = g^y mod p$ на основе АП-кода с параметрами $(2n, k, d)$.

7. Аутентификатор $\boldsymbol{u}_b$ передается корреспонденту *A*.

8. Корреспондент *A*, получив $Y = g^y mod p$ и используя вторые *n* бит своей последовательности $\boldsymbol{a}$, формирует местный аутентификатор $\boldsymbol{u}'_b$ и сравнивает его с аутентификатором $\boldsymbol{u}_b$, полученным от корреспондента *B*. Если число несовпадений символов для пары аутентификаторов $dist = \left| \boldsymbol{u}_b \oplus \boldsymbol{u}'_b \right|$ меньше некоторого порога Δ, значение *Y* признается подлинным.

Если значение *DH* обоими корреспондентами признаны подлинными, то корреспонденты *A* и *B* формируют общий ключ по методу Диффи — Хеллмана, то есть $K = (DH_B)^x = (DH_A)^y$. Тем самым установлена аутентичность ключа *K*.

Проведем анализ данного протокола в условиях атаки «человек посередине», когда нарушитель использует перехват-пересылку сообщений подобно тому, как это было рассмотрено при анализе протокола Magpairing (рисунок 6).

1. Корреспонденты *A* и *B*, подверженные атаке «человек посередине», формируют значения Диффи — Хеллмана совместно с нарушителем *E*.

2. Корреспонденты *A*, *B* и нарушитель *E* генерируют строки $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{e}$ из показаний их датчиков магнитометров.

3. Корреспондент *A* начинает процедуру аутентификации. Используя первые *n* бит последовательности $\boldsymbol{a}$, он формирует аутентификатор $\boldsymbol{u}_a$ длиной *n* бит для последовательности $X = g^x mod p$ на основе АП-кода с параметрами $(2n, k, d)$.

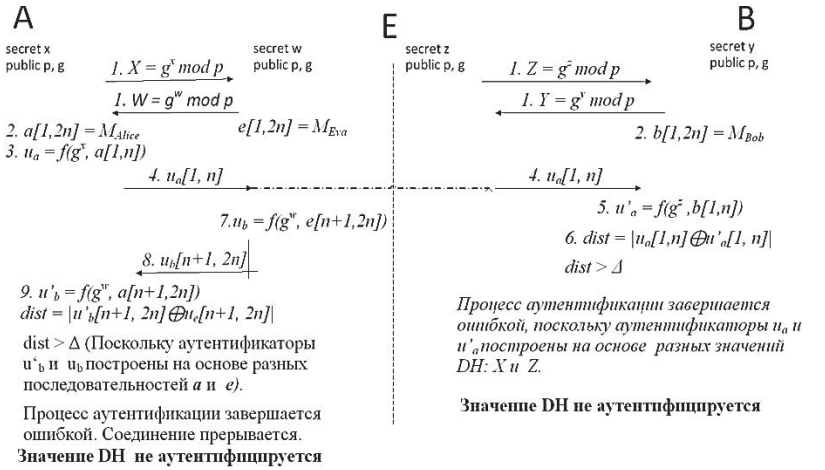

Рис.6. Протокол аутентификации ключей на основе аутентифицирующих помехоустойчивых кодов с использованием магнитометрических данных в условиях активного перехвата

4. Корреспондент *B*, получив аутентификаторы $\boldsymbol{u}_a$, формируют местные аутентификатор $\boldsymbol{u}'_a$ для значения DH Z, используя первую половину строки $\boldsymbol{b}$.

5. Корреспондент *B* проводит сравнение аутентификаторов, вычисляя хэмминговское расстояние между ними — $dist$. Так как при формировании аутентификаторов использовались разные значения DH, то с большой вероятностью $dist > \Delta$. Следовательно, значение DH Z не аутентифицируется.

6. Нарушитель *E* может инициировать процедуру аутентификации в сторону корреспондента *A*, имитируя *B*, формирует аутентификатор $\boldsymbol{u}_b[n+1, 2n] = f(g^w, \boldsymbol{e}[n+1, 2n]$ с использованием своей случайной строки $\boldsymbol{e}[1, 2\boldsymbol{n}]$.

7. Нарушитель *E* передает $\boldsymbol{u}_b$ корреспонденту A.

8. Корреспондент A, приняв $\boldsymbol{u}_b$, формирует местный аутентификатор $\boldsymbol{u}'_b[n+1, 2n] = f(g^w, \boldsymbol{a}[n+1, 2n]$ и сравнивает его с $\boldsymbol{u}_b[n+1, 2n]$. Так как аутентификаторы получены с использованием разных строк, то $dist > \Delta$. Процесс аутентификации завершается ошибкой.

Таким образом, аутентификация значения DH будет неудачной, независимо от того, какую стратегию выбирает нарушитель: ответ на запрос с использованием своих данных магнитометра или перехват — пересылка аутентификатора, принятого от корреспондента A корреспондентом *B*.

Заметим также, что нарушитель может применить атаку отражения. Для этого, получив от корреспондента А значение Диффи — Хеллмана $X = g^x mod p$, он посылает в ответ это же значение $W = X = g^x mod p$. Более того, он формирует аутентификатор, повторяя аутентификатор, который получил от А: $\boldsymbol{u}_b[1,n] = \boldsymbol{u}_a[1,n]$ (имитируя В). Однако и в этом случае нарушитель не достигнет цели, поскольку, согласно протоколу, в ответе должна использоваться вторая часть случайной последовательности.

Перейдем к количественной оценке данного протокола.

6. Оптимизация параметров АП-кодов для протокола аутентификации ключа с использованием магнитометрических данных. В [35] показано, что устойчивость к навязыванию ложных сообщений зависит от так называемого асимметричного кодового расстояния — d_{01} АП-кода, которое определяется числом переходов из 0 в 1 между кодовыми словами, соответствующими истинному m_i и ложному $\tilde{m}_i$ сообщениям.

Нахождение асимметричного кодового расстояния — сложная задача. Подоптимальный, хотя и не слишком экономичный способ построения (n_a, k_a) кода с известным d_{01} предложен в [34] и заключается в следующем.

Выберем некоторый (n,k) — код с известным минимальным расстоянием d. Заменим в каждом кодовом слове символ 1 на 10, а символ 0 на 01, получим (n_a, k_a) — АП-код с параметрами:

$$n_a = 2n, k_a = k, d_{01} = d, \tau = n. \quad (1)$$

Далее этот код используется для аутентификации блоков сообщений длиной k_a.

Основными характеристиками АП-кода являются:

P_f — вероятность ложного отклонения переданного сообщения, когда нарушитель не вмешивался в процесс передачи.

P_d — вероятность успешного навязывания ложного сообщения.

В [37] получены следующие соотношения для P_f и P_d:

$$P_f = \sum_{i=\Delta}^{2n_0} C_{2n_0}^i p_m^i (1-p_m)^{2n_0-1}, \quad (2)$$

$$P_d = \sum_{i=0}^{\Delta} C_d^i p_w^i (1-p_w)^{d-i} \sum_{j=0}^{\Delta-i} C_{2n_0-d}^j p_m^j (1-p_m)^{2n_0-d-j}, \quad (3)$$

где $p_m = p(a_i \neq b_i)$ — вероятность несовпадения бит в аутентифицирующих последовательностях ***a*** и ***b***, $p_w = p(a_i \neq e_i)$ — вероятность несовпадения бит в последовательности ***a*** и ***e***, где ***e*** — аутентифицирующая последовательность у нарушителя.

При выбранных k и n, параметр d может быть оценен с использованием границы Варшамова — Гильберта [35]:

$$\frac{k}{n} \geq 1 - g\left(\frac{n}{d}\right), \tag{4}$$

где $g(x) = -x\log x - (1-x)\log(1-x)$ — энтропийная функция.

Рассмотрим сначала частный случай применения АП-кода для аутентификации значений DH, когда значение DH аутентифицируется одним аутентификатором.

Будем полагать, что в нашем случае p_w =1/2, поскольку при формировании магнитометрических данных мобильные устройства законных пользователей находятся рядом, а устройство нарушителя удалено от них. В качестве примера на рисунке 7 показаны зависимости $P_f(\Delta)$ и $P_d(\Delta)$ для (128,32,28) — АП-кода при разных значений p_m, рассчитанные согласно (2), (3).

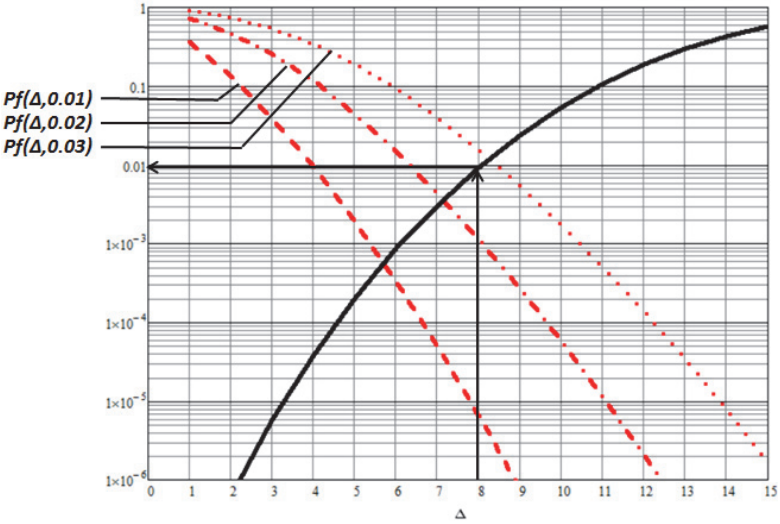

Рис. 7. Зависимости P_f *(штриховая линия)* P_d *(сплошная линия)* от порога Δ при разных значениях вероятности несовпадения аутентифицирующих последовательностей

Видим, что P_f убывает при увеличении порога Δ и уменьшении p_m (штриховая линия). Наоборот вероятность навязывания ложного ключа увеличивается с увеличением Δ (сплошная линия). Выбирая значение порога Δ, можно обеспечить требуемую величину вероятности ложного отклонения блока P_f. При этом же значении порога получаем P_d.

При аутентификации значения DH, представленного последовательностью большой длины, потребуется использование кода большой длины, для которого сложно найти минимальное хэмминговское расстояние *d*. Поэтому рассмотрим общий случай, когда аутентификация значения DH проводится по частям. Для этого аутентифицируемая последовательность разбивается на блоки равной длины и каждый блок аутентифицируется отдельно. Протокол аутентификации в этом случае будет выглядеть так:

1. Корреспондент *A* формирует значение Диффи — Хеллмана $DH_A = \boldsymbol{\alpha}^{\mathbf{x}}$. Это значение представляется в виде двоичной последовательности длиной *L* бит. Последовательность разделяется на *N* блоков длиной *k* бит каждый.

2. Используя свои магнитометрические данные (последовательность $\boldsymbol{a}$), корреспондент A формирует аутентификаторы $\boldsymbol{u}_{ai}$ длиной *n* бит на основе АП-кода с параметрами $(2n, k, d)$ для каждого *i*-го подблока, $i = 1, 2, ..., N$. Заметим, что для формирования очередного аутентификатора используется новая часть последовательности $\boldsymbol{a}$.

3. Значение DH_A и аутентификаторы $\boldsymbol{u}_{ai}$, передаются корреспонденту *B*.

4. Корреспондент *B*, получив DH_A и используя свои магнитометрические данные (последовательность $\boldsymbol{b}$), формирует местные аутентификаторы $\boldsymbol{u}'_{ai}$ и сравнивает их с аутентификаторами $\boldsymbol{u}_{ai}$, которые получил от корреспондента *A* в порядке их поступления. Если число несовпадений символов для пары аутентификаторов $\left|\boldsymbol{u}_{ai} \oplus \boldsymbol{u}'_{ai}\right|$ меньше некоторого порога Δ, блок признается подлинным.

После этого аналогичным порядком проводится аутентификация значения Диффи — Хеллмана DH_B, передаваемого от *B* к *A*. Значение Диффи — Хеллмана *DH* корреспондента признается подлинными в целом, если аутентифицирован каждый блок.

Если значение *DH* обоими корреспондентами признаны подлинными, то корреспонденты *A* и *B* формируют общий ключ по способу Диффи — Хеллмана, то есть:

$$K = (DH)^x = (DH)^y . \quad (4)$$

Вероятность ложного отклонения значения *DH* корреспондентом имеет место, если произойдет ложное отклонение хотя бы одного блока.

$$P_f(DH) = 1 - (1 - P_f)^N . \quad (5)$$

Ложная аутентификация, то есть навязывание нарушителем ложного значения Диффи — Хеллмана будет иметь место, если будут успешно навязаны все *n* блоков и соответствующие им аутентификаторы. Вероятность этого события:

$$P_d(DH) = (P_d)^N . \quad (6)$$

Для формирования аутентификаторов требуется аутентифицирующая последовательность длиной $l = n_a N$.

Выбор наилучшего кода представляет самостоятельную научную задачу, которая может быть сформулирована следующим образом. Заданы: длина значения DH — n_0, допустимая вероятность ложного отклонения — $P_f^{доп}(DH)$, допустимая вероятность навязывания — $P_d^{доп}(DH)$. Требуется выбрать: параметры АП-кода: (n_a, k_a, d_{01}) и порог Δ, для которых минимизируется длина аутентифицирующей последовательности (*l*) и выполняются требования по вероятности навязывания ложного ключа и вероятности ложного отклонения истинного ключа, то есть:

$$P_f(DH) \le P_f^{доп}(DH), \;\; P_d(DH) \le P_d^{доп}(DH) , \quad (7)$$

$$l \to min . \quad (8)$$

Необходимость минимизации величины *l* мы объясняем тем, что корреспонденты *A* и *B* могут иметь возможность проходить процедуру сопряжения (рисунок 1) редко, поэтому выработанная аутентифицирующая последовательность должна иметь длину, достаточную для многократной аутентификации ключей между процедурами сопряжения.

В [36] предложен следующий подход к оптимизации параметров системы аутентификации. Фиксируется скорость кода $R = k_a / n_a$. Рассчитываются на основе (2), (3) параметры $P_f, P_d, P_f(DH), P_d(DH)$ для разных порогов Δ и разных длин кодов этой скорости. Затем, среди

этих кодов отбираются те, которые удовлетворяют условию (7). Наконец, среди отобранных кодов, имеющих разные скорости, выбирается код, для которого аутентифицирующая последовательность имеет минимальную длину (8).

В таблицах 2-5 приведены значения $P_f, P_d, P_d(DH)$ для кодов, имеющих скорости R=1/2, 1/3,1/4,1/5 для разных длин кодовых блоков при p_m=0,01 и длине ключа n_0=256 бит. Значения вероятности P_f(DH) для всех случаев было задано равным 10^{-6}. Серым цветом помечены коды, для которых выполняются условия $P_f(DH) = 10^{-6}$, $P_d(DH) \le 10^{-6}$.

Таблица 2. Вероятности $P_f, P_d, P_d(DH)$, для разных значений параметров аутентифицирующих кодов со скоростью R=05

Код n,k	16,8	32,16	64,32	128,64	256,128	512,256
Δ	5	6	8	10	13	19
P_f	3.1×10^{-8}	6.2×10^{-8}	1.2×10^{-7}	2.5×10^{-7}	5×10^{-7}	10-6
P_d	1	1	1	0.9	0.2	8×10^{-4}
$P_d(DH)$	1	1	1	0,656	0.04	8×10^{-4}
Длина аутентифицирующей последовательности L=512 бит						

Таблица 3. Вероятности $P_f, P_d, P_d(DH)$, для разных значений параметров аутентифицирующих кодов со скоростью *R=1/3*

Код n,k	24,8	48,16	96,32	192,64	384,128	512,256
Δ	6	7	9	12	16	24
P_f	3.1×10^{-8}	6.2×10^{-8}	1.2×10^{-7}	2.5×10^{-7}	5×10^{-7}	10^{-6}
P_d	1	0.85	0.6	0.02	5×10^{-7}	10^{-17}
$P_d(DH)$	1	0.074	0.017	1.6×10^{-7}	2.5×10^{-13}	10^{-17}
Длина аутентифицирующей последовательности L=768 бит.						

Приведенные примеры показывают, что наилучшим вариантом аутентификации ключа длиной 256 бит при вероятности несовпадения последовательностей магнитометров p_m=0.01 является выбор кода со скоростью $R=1/3$ с параметрами (128,32). При этом обеспечивается:

– вероятность навязывания ложного ключа — $P_d(DH)=3{,}9\cdot10^{-9}$;

– вероятность ложного отклонения ключа — $P_f(DH)=10^{-6}$.

Ключ аутентифицируется по блокам длиной 32 бита. Для аутентификации расходуется 768 бит последовательности, полученной от магнитометрического датчика во время процедуры сопряжения мобильных устройств.

Таблица 4. Вероятности, $P_f, P_d, P_d(DH)$ для разных значений параметров аутентифицирующих кодов со скоростью R=1/4

Код n,k	32,8	64,16	128,32	256,64	512, 128	1024, 256
Δ	6	8	10	14	19	28
P_f	3.1×10^{-8}	6.2×10^{-8}	1.2×10^{-7}	2.5×10^{-7}	5×10^{-7}	10^{-6}
P_d	1	0.7	0.05	3×10^{-5}	10^{-14}	10^{-35}
$P_d(DH)$	1	3.3×10^{-3}	3.9×10^{-11}	8.1×10^{-19}	10^{-28}	10^{-35}
Длина аутентифицирующей последовательности L=1024 бит						

Таблица 5. Вероятности, $P_f, P_d, P_d(DH)$ для разных значений параметров аутентифицирующих кодов со скоростью R=1/5

Код n,k	40,8	80,16	160,32	320,64	640, 128	1280, 256
Δ	7	9	11	15	21	33
P_f	3.1×10^{-8}	6.2×10^{-8}	1.2×10^{-7}	2.5×10^{-7}	5×10^{-7}	10^{-6}
P_d	0.85	0.35	1.5×10^{-3}	10^{-9}	10^{-24}	10^{-55}
$P_d(DH)$	0.074	5×10^{-8}	2.5×10^{-23}	10^{-36}	10^{-48}	10^{-55}
Длина аутентифицирующей последовательности равна L=1280 бит.						

Приведенные примеры выбора параметров кодов показывают реализуемость способа и эффективность в смысле «расхода» аутентифицирующей последовательности, выработанной на этапе сопряжения устройств.

7. Заключение. Широкое распространение мобильных беспроводных устройств (смартфонов, планшетов и пр.) остро ставит вопрос о криптографической защите передаваемой этими устройствами информации, что, в свою очередь, требует обеспечения устройств ключами и решения задачи их аутентификации. В работе решается задача аутентификации распределяемых по методу Диффи —Хеллмана ключей для мобильных устройств в рамках сценария сопряжения мобильных устройств. В этих условиях устройства, формирующие ключ, располагаются близко друг к другу, вплоть до физического контакта между ними. Для аутентификации создается дополнительный канал обмена данными. Проведенный анализ дополнительных каналов — визуального, акустического, вибрационного, тактильного, магнитометрического — выявил преимущества последнего по скорости и достоверности аутентификации, а также удобству использования этого канала по сравнению с другими.

Магнитометрический канал образуется при наличии в мобильных устройствах магнитометров (небольших узлов объемом несколько $мм^3$), которые измеряют магнитное поле Земли. Случайные колебания магнитного поля в точке измерения позволяют получить в двух мобильных устройствах совпадающие с большой вероятностью случайные последовательности, которые могут быть использованы для аутентификации сеансовых ключей.

В работе проведен детальный анализ протокола аутентификации ключей Magparing, формируемых по методу Диффи — Хеллмана, предложенный в [20], который показал уязвимость этого протокола к атаке «человек-посередине». Уязвимость протокола также подтверждена на основе использования программы анализа безопасности протоколов AVISPA.

Предложен безопасный способ аутентификации ключей (значений Диффи — Хеллмана) на основе аутентифицирующих помехоустойчивых кодов (АП-кодов). Аутентификаторы для значений Диффи-Хеллмана формируются на основе и блоков АП-кода и случайных последовательностей, полученных из показаний магнитометров. Предложен подход к оптимизации параметров АП-кода, обеспечивающего выполнение требований по вероятности ложного отклонения и вероятности навязывания ключа заданной длины при минимизации длины цепочки магнитометрических данных, расходуемых в процедуре аутентификации.

В качестве примера показано, что при вероятности несовпадения цепочек бит магнитометрических данных, равной 0.01, ключ длиной 256 бит может быть аутентифицирован с вероятностью навязывания не более 10^{-9} и вероятностью ложного отклонения 10^{-6} при использовании помехоустойчивого кода с параметрами (128,32). При этом требуемая длина цепочки магнитометрических данных составит 768 бит. Данный пример подтверждает возможность достаточно эффективной реализации предложенного способа аутентификации ключей, распределяемых методом Диффи — Хеллмана.

Автор выражает благодарность Зуевой Е.О. за проведение исследований протокола Magparing с помощью программы AVISPA.

Литература

1. Конфиденциальная сотовая связь (официальный сайт Мегафон). URL: www.spb.megafon.ru (дата обращения: 25.02.2019).
2. *Ferguson N., Schneier B.* Practical Cryptography // New York: Wiley. 2003. vol. 142. 333 p.
3. RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and Certification Revocation List(CRL) Profile. URL: https://tools.ietf.org (дата обращения: 23.02.2019).
4. *Mukherjee A., Fakoorian S.A.A., Huang J., Swindlehurst A.L.* Priciples of Physical Layer Security in Multiuser Wireless Networks: A Survey // IEEE Communications Surveys & Tutorials. 2014. vol. 16. no. 3. pp. 1550–1573.
5. *Zeng K.* Physical Layer Key Generation in Wireless Networks. Challenges and Opportunities // IEEE Communications Magazine. 2015. vol. 53. no. 6. pp. 33–39.
6. *Zhang J., Duong T.Q., Marshall A., Woods R.* Key Generation from Wireless Channels: a Review // IEEE Access. 2016. vol. 4. pp. 614–626.
7. *Huth C. et al.* Information reconciliation schemes in physical-layer security: A survey // Computer Networks. 2016. vol. 109. pp. 84–104.
8. *Dean T.R, Goldsmith A.J.* Physical-layer Cryptography through Massive MIMO // IEEE Transactions on Information Theory. 2017. vol. 63. no. 8. pp. 5419–5436.
9. *Steinfeld R., Sakzad A.* On Massive MIMO Physical Layer Cryptosystem // 2015 IEEE Information Theory Workshop-Fall. 2015. pp. 292–296.
10. *Yakovlev V., Korzhik V., Mylnikov P., Morales-Luna G.* Secret Key Agreement Based on a Communication through Wireless MIMO Fading Channels // 2016 Federated Conference on Computer Science and Information Systems. 2016. pp. 823–830.
11. *Yakovlev V., Korzhik V., Mylnikov P., Morales-Luna G.* Outdoor Secret Key Agreement Scenarios Using Wireless MIMO Fading Channels // International Journal of Computer Science and Applications. 2017. vol. 1. no. 1. pp. 1–25.
12. *Qin D., Ding Z.* Exploiting Multi-Antenna Non-Reciprocal Channels for Shared Secret Key Generation // IEEE Transactions on Information Forensics and Security. 2016. vol. 11. no. 12. pp. 2691–2705.
13. *Zhang J. et al.* Experimental Study on Channel Reciprocity in Wireless Key Generation // 2016 17th IEEE International Workshop on Signal Processing Advances Wireless Communications (SPAWC). 2016. pp. 1–5.
14. *Korzhik V. et al.* Secret Key Sharing Protocol Between Units Connected by Wireless MIMO Fading Channel // 2018 Federated Conference on Computer Science and Information Systems (FedCSIS-2018). 2018. pp. 569–576.
15. *Ding Y., Zhang J., Fisco V.F.* Retrodirective-Assisted Secure Wireless Key Establishment // IEEE Transactions on Communication. 2016. vol. 65. no. 1. pp. 320–334.

16. *Mirzadeh S., Cruickshank H., Tafazolli R.* Secure Device Pairing: A Survey // IEEE Communications Surveys & Tutorials. 2013. vol. 16. no. 1. pp. 17–40.
17. *Jokela T., Chong M.K., Lucero A., Gellersen H.* Connecting Devices for Collaborative Interaction // Interactions. 2015. vol. 22. no. 4. pp. 39–43.
18. *Nourreen A., Shoaib U., Sarfraz M.S.* Securre Device Pairing Methods: An Overview // International Journal of Advanced Computer Science and Application. 2017. vol. 8. no. 9. pp. 442–451.
19. *Diffe M., Hellman M.* New directions in cryptography // IEEE Transactions on Information Theory. 1976. vol. 22. no. 6. pp. 644–654.
20. *Jin R. et al.* Magpairing: Pairing Smartphones in Close Proximity Using Magnetometer // IEEE Transactions on Information Forensics and Security. 2016. vol. 11. no. 6. pp. 1304–1319.
21. *McCune J.M., Perring A., Reiter M.K.* Seeing-is-Believing: Using Camera Phones for Human-Verifiable Authentication // 2005 IEEE Symposium on Security and Privacy (S&P'05). 2005. pp.110–124.
22. *Saxena N., Ekberg J.E., Kostiainen K., Asokan N.* Secure Device Pairing Based on a Visual Channel // 2006 IEEE Symposium on Security and Privacy (S&P'06). 2006. 6 p.
23. *Prasad R., Saxena N.* Efficient Device Pairing Using "Human-Comparable" Synchronized Audiovisual Patterns // International Conference on Applied Cryptography and Network Security. 2008. pp. 328–345.
24. *Goodrich M. T. et al.* Using Audio in Secure Device Pairing // International Journal of Security and Networks. 2009. vol. 4. no. 1-2. pp. 57–68.
25. *Goodrich M.T. et al.* Loud and Clear: Human-Verifiable Authentication Based on Audio // 26th IEEE International Conference on Distributed Computing Systems. ICDCS. 2006. pp. 1–10.
26. *Soriente C., Tsudik G., Uzun E.* HAPADEP: Human-Assisted Pure Audio Device Pairing // International Conference on Information Security. 2008. pp. 385–400.
27. *Roy N., Choudhury R.R.* Ripple {II}*:* Faster Communication through Physical Vibration // 12th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16). 2016. pp. 671–684.
28. *Mayrhofer R., Gellersen H.* Shake Well Before Use: Intuitive and Secure Pairing of Mobile Devices // IEEE Transactions on Mobile Computing. 2009. vol. 8. no. 6. pp. 792–806.
29. *Soriente C., Tsudik G., Uzun E.* BEDA: Button-Enabled Device Association // International Workshop on Security for Spontaneous Interaction (IWSSI). 2007. pp. 443–449.
30. *Kumar A., Saxena N., Tsudik G., Uzun E.* A Comparative Study of Secure Device Pairing Methods // Pervasive and Mobile Computing. 2009. vol. 5. no. 6. pp. 734–749.
31. *Корпусов В.Д., Ольховой О.О., Яковлев В.А.* Исследование датчика случайных чисел на основе магнитометра // VIII Международная научно-техническая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (АПИНО-2018). 2018. С. 488–493.
32. *Котенко И.В., Резник С.А., Шоров А.В.* Верификация протоколов безопасности на основе комбинированного использования существующих методов и средств // Труды СПИИРАН. 2009. Вып. 8. С. 293–310.
33. *Зуева Е.О., Яковлев В.А.* Анализ стойкости способа аутентификации для протокола распределения ключей на основе магнитометрических данных с помощью программы AVISPA // VIII Международная научно-техническая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (АПИНО-2018). 2018. С. 392–396.
34. *Maurer U.* Information-Theoretically Secure Secret-Key Agreement by not Authenticated Public Discussion // International Conference on the Theory and Applications of Cryptographic Techniques. 1997. pp. 209–225.

35. *Korzhik V., Yakovlev V., Morales-Luna G., Chesnokov R.* Perfomance Evaluation of Keyless Authentication Based on Noisy Channel // International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security. 2007. pp. 115–126.
36. *Зуева Е.О., Яковлев В.А.* Разработка способа помехоустойчивой аутентификации для протокола распределения ключей Диффи-Хеллмана на основе магнитометрических данных // VIII Международная научно-техническая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (АПИНО-2018). 2018. С. 401–406.
37. *MacWilliams F.J., Sloane N.J.A.* The Theory of Error Correcting Codes // Elsevier. 1977. vol. 16. 762 p.

Яковлев Виктор Алексеевич — д-р техн. наук, профессор, профессор, кафедра защищенных систем связи, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича (СПбГУТ). Область научных интересов: информационная безопасность, криптография. Число научных публикаций — 150. viyak@bk.ru; пр. Большевиков, 22, 193232, Санкт-Петербург, Российская Федерация; р.т.: +7(911)1455359.

DOI 10.15622/sp.2019.18.3.705-740

V.A. YAKOVLEV

AUTHENTICATION OF KEYS DISTRIBURTED BY THE DIFFIE-HELLMAN METHOD FOR MOBILE DEVICES BASED ON AUTHENTICATION CODES AND MAGNETOMETRIC DATA

Yakovlev V.A. **Authentication of Keys Distributed by the Diffie-Hellman Method for Mobile Devices based on Authentication Codes and Magnetometric Data.**

Abstract. The wide distribution of mobile wireless devices (smartphones, tablets, etc.) warrants cryptographic protection of information transmitted by these devices, which requires supplying these devices with keys and providing their authentication. Recently, research on key authentication methods within scenarios of pairing mobile devices, has been increasingly relevant. In these conditions, mobile devices are located close to each other, up to the physical contact, and an additional key sharing authenticated channel protected from interception is established for purposes of key authentication.

The analysis of additional channel versions: visual, acoustic, vibration, tactile, and magnetometric shows advantages of the latter one in terms of speed and reliability of authentication, as well as easer se of this channel compared to other methods. A magnetometer channel forms if there are magnetometers in mobile devices that measure the Earth's magnetic field. Random fluctuations of the magnetic field at the measurement point allow to generate in a pair of mobile devices random sequences that coincide with a high probability and which can be used to authenticate session keys.

The "Magparing" protocol of mobile devices keys authentication, which are distributed by Diffie-Hellman method is studied. his protocol is based on the magnetometer data measuring. We demonstrate that the protocol is succeptible to "man-in-the-middle" attack. This fact is confirmed also by software AVISPA simulation.

A new key authentication method based on the use of authenticating code (A-code) is proposed. Authenticators for Diffie-Hellman values are generated based on A-code blocks and random sequences obtained by the reading of magnetometer's values. An approach for A-code parameters optimization, that conforms to the requirements for authentication key length and both to the probabilities of false key removal and false key deception, is investigated. We present an example of code parameters for key authentication with the length of 256 bits, providing the probability of a false key agreement of not greater than 10-9 and a probability of false rejection of a true key equal to –10–6, which shows viability of the proposed authentication method.

Key words: Authentication, Key Distribution, Diffie-Hellman Method, Side Authentication Channel, Magparing Protocol, Authenticating Codes.

Yakovlev Viktor Alekseevich — Ph.D., Dr.Sci., Professor, Professor, Department of Secure Means of Communication, The Bonch-Bruevich Saint-Petersburg State University of Telecommunications. Research interests: information security, cryptography. The number of publications — 150. viyak@bk.ru; 22, pr. Bolshevikov, 193232, St. Petersburg, Russian Federation; office phone: +7(911)1455359.

References

1. Konfidencial'naya sotovaya svyaz. (oficial'nyj sait Megafon). [*Confidential cellular* (official web site of Megafon)]. Available at: www.spb.megafon.ru. (accessed: 25.02.2019). (In Russ).
2. Ferguson N., Schneier B. Practical Cryptography. New York: Wiley. 2003. vol. 142. 333 p.

3. RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and Certification Revocation List(CRL) Profile. Available at: https://tools.ietf.org (accessed: 23.02.2019).
4. Mukherjee A., Fakoorian S.A.A., Huang J., Swindlehurst A.L. Priciples of Physical Layer Security in Multiuser Wireless Networks: A Survey. *IEEE Communications Surveys & Tutorials*. 2014. vol. 16. no. 3. pp. 1550–1573.
5. Zeng K. Physical Layer Key Generation in Wireless Networks. Challenges and Opportunities. *IEEE Communications Magazine*. 2015. vol. 53. no. 6. pp. 33–39.
6. Zhang J., Duong T.Q., Marshall A., Woods R. Key Generation from Wireless Channels: a Review. *IEEE Access*. 2016. vol. 4. pp. 614–626.
7. Huth C. et al. Information reconciliation schemes in physical-layer security: A survey. *Computer Networks*. 2016. vol. 109. pp. 84–104.
8. Dean T.R, Goldsmith A.J. Physical-layer Cryptography through Massive MIMO. *IEEE Transactions on Information Theory*. 2017. vol. 63. no. 8. pp. 5419–5436.
9. Steinfeld R., Sakzad A. On Massive MIMO Physical Layer Cryptosystem. 2015 IEEE Information Theory Workshop-Fall. 2015. pp. 292–296.
10. Yakovlev V., Korzhik V., Mylnikov P., Morales-Luna G. Secret Key Agreement Based on a Communication through Wireless MIMO Fading Channels. 2016 Federated Conference on Computer Science and Information Systems. 2016. pp. 823–830.
11. Yakovlev V., Korzhik V., Mylnikov P., Morales-Luna G. Outdoor Secret Key Agreement Scenarios Using Wireless MIMO Fading Channels. *International Journal of Computer Science and Applications.* 2017. vol. 1. no. 1. pp. 1–25.
12. Qin D., Ding Z. Exploiting Multi-Antenna Non-Reciprocal Channels for Shared Secret Key Generation. *IEEE Transactions on Information Forensics and Security*. 2016. vol. 11. no. 12. pp. 2691–2705.
13. Zhang J. et al. Experimental Study on Channel Reciprocity in Wireless Key Generation. 2016 17th IEEE International Workshop on Signal Processing Advances Wireless Communications (SPAWC). 2016. pp. 1–5.
14. Korzhik V.et al. Secret Key Sharing Protocol Between Units Connected by Wireless MIMO Fading Channel. 2018 Federated Conference on Computer Science and Information Systems (FedCSIS-2018). 2018. pp. 569–576.
15. Ding Y., Zhang J., Fisco V.F. Retrodirective-Assisted Secure Wireless Key Establishment. *IEEE Transactions on Communication*. 2016. vol. 65. no. 1. pp. 320–334.
16. Mirzadeh S., Cruickshank H., Tafazolli R. Secure Device Pairing: A Survey. *IEEE Communications Surveys & Tutorials.* 2013. vol. 16. no. 1. pp. 17–40.
17. Jokela T., Chong M.K., Lucero A., Gellersen H. Connecting Devices for Collaborative Interaction. *Interactions*. 2015. vol. 22. no. 4. pp. 39–43.
18. Nourreen A., Shoaib U., Sarfraz M.S. Securre Device Pairing Methods: An Overview. *International Journal of Advanced Computer Science and Application*. 2017. vol. 8. no. 9. pp. 442–451.
19. Diffe M., Hellman M. New directions in cryptography. *IEEE Transactions on Information Theory.* 1976. vol. 22. no. 6. pp. 644–654.
20. Jin R. et al. Magpairing: Pairing Smartphones in Close Proximity Using Magnetometer. *IEEE Transactions on Information Forensics and Security*. 2016. vol. 11. no. 6. pp. 1304–1319.
21. McCune J.M., Perring A., Reiter M.K. Seeing-is-Believing: Using Camera Phones for Human-Verifiable Authentication. 2005 IEEE Symposium on Security and Privacy (S&P'05). 2005. pp. 110–124.
22. Saxena N., Ekberg J.E., Kostiainen K., Asokan N. Secure Device Pairing Based on a Visual Channel. 2006 IEEE Symposium on Security and Privacy (S&P'06). 2006. 6 p.
23. Prasad R., Saxena N. Efficient Device Pairing Using "Human-Comparable" Synchronized Audiovisual Patterns. International Conference on Applied Cryptography and Network Security. 2008. pp. 328–345.

24. Goodrich M. T. et al. Using Audio in Secure Device Pairing. *International Journal of Security and Networks.* 2009. vol. 4. no. 1-2. pp. 57–68.
25. Goodrich M.T. et al. Loud and Clear: Human-Verifiable Authentication Based on Audio. 26th IEEE International Conference on Distributed Computing Systems. ICDCS. 2006. pp. 1–10.
26. Soriente C., Tsudik G., Uzun E. HAPADEP: Human-Assisted Pure Audio Device Pairing. International Conference on Information Security. 2008. pp. 385–400.
27. Roy N., Choudhury R.R. Ripple {II}*:* Faster Communication through Physical Vibration. 12th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16). 2016. pp. 671–684.
28. Mayrhofer R., Gellersen H. Shake Well Before Use: Intuitive and Secure Pairing of Mobile Devices. *IEEE Transactions on Mobile Computing*. 2009. vol. 8. no. 6. pp. 792–806.
29. Soriente C., Tsudik G., Uzun E. BEDA: Button-Enabled Device Association. International Workshop on Security for Spontaneous Interaction (IWSSI). 2007. pp. 443–449.
30. Kumar A., Saxena N., Tsudik G., Uzun E. A Comparative Study of Secure Device Pairing Methods. *Pervasive and Mobile Computing*. 2009. vol. 5. no. 6. pp. 734–749.
31. Korpusov V.D., Yakovlev V.A., Ol'hovoj O.O. [Magnetometer based random number sensor analysis]. *VIII Mezhduarodnaya nauchno-tehnicheckaya konferenciya. Aktual'nye problemy infotelecommunikacij v nauke i obrazovanii (APINO-2018)* [VIII International Conference on Advanced Infotelecommunication (ICAIT-2018)]. 2018. pp. 488–493. (In Russ.).
32. Kotenko I.V., Reznik S.A., Shorov A.V. [Security Protocols Verification Combining Existing Approaches and Tools]. *Trudy SPIIRAN – SPIIRAS Proceedings.* 2009. vol. 8. pp. 293–310. (In Russ.).
33. Zueva E., Yakovlev V. [Analysis of the strength of the authentication method for the key distribution protocol based on magnetometric data using the AVISPA program]. *VIII Mezhduarodnaya nauchno-tehnicheckaya konferenciya. Aktual'nye problemy infotelecommunikacij v nauke i obrazovanii (APINO-2018)* [VIII International Conference on Advanced Infotelecommunication (ICAIT-2018)]. 2018. pp. 392–396. (In Russ.).
34. Maurer U. Information-Theoretically Secure Secret-Key Agreement by not Authenticated Public Discussion. International Conference on the Theory and Applications of Cryptographic Techniques. 1997. pp. 209–225.
35. Korzhik V., Yakovlev V., Morales-Luna G., Chesnokov R. Perfomance Evaluation of Keyless Authentication Based on Noisy Channel. International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security. 2007. pp. 115–126.
36. Yakovlev V., Zueva E. [Development of the robast authentication method for the Diffe-Hellman key distribution protocol based on magnetometric data] *VIII Mezhduarodnaya nauchno-tehnicheckaya konferenciya. Aktual'nye problemy infotelecommunikacij v nauke i obrazovanii (APINO-2018)* [VIII International Conference on Advanced Infotelecommunication (ICAIT-2018)]. 2018. pp. 401–406. (In Russ.).
37. MacWilliams F.J., Sloane N.J.A. The Theory of Error Correcting Codes. Elsevier. 1977. vol. 16. 762 p.