Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1366

(09/2020)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасные приложения и услуги (2) –
Безопасность интернета вещей (IoT)

Схемы совокупной аутентификации сообщений для среды интернета вещей

Рекомендация МСЭ-Т X.1366

ITU-T

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (1)	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности (1)	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (2)	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1319
Безопасность "умных" электросетей	X.1330–X.1339
Сертифицированная электронная почта	X.1340–X.1349
Безопасность интернета вещей (IoT)	**X.1360–X.1369**
Безопасность интеллектуальных транспортных систем (ИТС)	X.1370–X.1379
Безопасность технологии распределенного реестра	X.1400–X.1429
Безопасность технологии распределенного реестра	X.1430–X.1449
Протоколы безопасности (2)	X.1450–X.1459
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699
КВАНТОВАЯ СВЯЗЬ	
Терминология	X.1700–X.1701
Квантовый генератор случайных чисел	X.1702–X.1709
Структура безопасности QKDN	X.1710–X.1711
Проектирование безопасности QKDN	X.1712–X.1719
Методы обеспечения безопасности QKDN	X.1720–X.1729
БЕЗОПАСНОСТЬ ДАННЫХ	
Безопасность больших данных	X.1750–X.1759
БЕЗОПАСНОСТЬ СЕТЕЙ 5G	X.1800–X.1819

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т X.1366

Схемы совокупной аутентификации сообщений для среды интернета вещей

Резюме

Количество устройств интернета вещей (IoT) возрастает, и в ближайшем будущем огромное число устройств будет подключено к сети IoT, включая 5G. В Рекомендации МСЭ-Т X.1366 определены две схемы аутентификации сообщений. Первая – схема совокупной аутентификации сообщений (AMA) для IoT, которая служит базовым механизмом. Вторая – схема интерактивной совокупной аутентификации сообщений (IAMA) с интерактивным протоколом в упрощенном и безопасном режиме. Обе схемы совокупной аутентификации сообщений могут применяться для обеспечения аутентификации объекта (личности), а также для обеспечения аутентификации сообщений. Эти схемы, возможно, неприменимы во всех сценариях использования устройств IoT, но они достаточно эффективны и пригодны для сценариев использования в следующих условиях:

- требуется аутентификация сообщений от десятков до десятков тысяч устройств IoT;
- данные или сообщения обрабатываются для процесса аутентификации, который происходит часто и периодически.

Например типовыми возможными сценариями использования таких схем являются приложения наблюдения для использования данных изображения и дистанционная телеметрия, как например мониторинг работы завода или фабрики и мониторинг состояния здоровья.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1366	03.09.2020 г.	17-я	11.1002/1000/14262

Ключевые слова

Совокупная аутентификация сообщений (AMA), IoT.

* Для доступа к Рекомендации наберите в адресном поле вашего веб-навигатора URL http://handle.itu.int/, после которого укажите уникальный идентификатор Рекомендации. Например: http://handle.itu.int/11.1002/1000/11830-en.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" (shall) или некоторые другие обязывающие выражения, такие как "обязан" (must), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т X.1366

Схемы совокупной аутентификации сообщений для среды интернета вещей

1 Сфера применения

В настоящей Рекомендации определены две схемы аутентификации сообщений. Первая – схема совокупной аутентификации сообщений (AMA) для IoT, которая служит базовым механизмом. Вторая – схема интерактивной совокупной аутентификации сообщений (IAMA) с интерактивным протоколом в упрощенном и безопасном режиме. Обе схемы совокупной аутентификации сообщений могут применяться для обеспечения аутентификации объекта (личности), а также для обеспечения аутентификации сообщений.

Способы реализации этих схем в конкретной среде IoT, а также технологии совокупной подписи выходят за рамки данной Рекомендации.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие справочные документы могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используется следующий термин, определенный в других документах:

3.1.1 код аутентификации сообщения (message authentication code (MAC)) [b-ITU-T X.813]: Криптографическое контрольное значение, используемое для аутентификации источника и целостности данных.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины:

3.2.1 аутентификация сообщения (message authentication): Свойство, которое гарантирует, что сообщение не было изменено во время передачи, обеспечивает целостность данных и позволяет принимающей стороне проверить источник сообщения.

3.2.2 совокупная аутентификация сообщений (aggregate message authentication (AMA)): Свойство, позволяющее объединять несколько кодов аутентификации сообщений, генерированных несколькими отправителями, в более короткий код аутентификации, который может быть проверен получателем, располагающим секретными ключами отправителей.

3.2.3 аутентификационные признаки (authentication tags): Элементы данных, используемые для аутентификации сообщений.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

AGT	Adaptive Group Testing protocol	Протокол адаптивного группового тестирования
AMA	Aggregate Message Authentication	Совокупная аутентификация сообщений
AMAC	Aggregate Message Authentication Code	Код совокупной аутентификации сообщений
IAMA	Interactive Aggregate Message Authentication	Интерактивная совокупная аутентификация сообщений
IoT	Internet of Things	Интернет вещей
MAC	Message Authentication Code	Код аутентификации сообщения
XOR	Exclusive OR operation	Операция "исключающее ИЛИ"

5 Соглашения

Отсутствуют.

6 Обзор и базовая концепция

6.1 Обзор

Количество устройств интернета вещей (IoT) постоянно возрастает, и в ближайшем будущем к сетям IoT, в том числе 5G, будет подключено огромное число устройств. В настоящей Рекомендации представлена упрощенная и надежная система аутентификации, которая может применяться в такой ситуации.

Код аутентификации сообщения (MAC) – это один из наиболее фундаментальных криптографических примитивов, и его можно использовать в качестве простого криптографического примитива для аутентификации сообщений. Однако, как показано на рисунке 1, в современных системах IoT аутентификационные признаки (см. пункт 3.2.3) сообщений, отправляемых устройствами IoT, генерируются индивидуально на стороне устройства IoT, и каждое сообщение со сгенерированным признаком обычно проверяется в ходе осуществляемого на стороне получателя процесса проверки. Основная проблема этого современного сценария IoT заключается в том, что нагрузка на процессы аутентификации и проверки увеличивается пропорционально росту количества устройств IoT.

Код совокупной аутентификации сообщений (AMAC) – это известная технология, позволяющая сжимать несколько признаков MAC нескольких генерированных разными устройствами сообщений в один совокупный признак без ущерба для безопасности (см. Дополнение II). Преимущество AMAC заключается в том, что размер совокупного признака намного меньше общего размера признаков MAC и, следовательно, он будет полезен в применениях сетей подвижной связи или сетей IoT со множеством подключенных устройств, отправляющих сообщения. В частности, AMAC можно использовать для повышения эффективности сетей в применениях, где используются MAC. Однако этот метод не позволяет выявлять недействительные сообщения среди множества сообщений, когда при использовании совокупного признака AMAC эти сообщения в целом признаны недействительными. В настоящей Рекомендации существующая схема AMAC расширена таким образом, что она позволяет сжимать несколько признаков MAC с возможностью обнаружения отдельных недействительных сообщений.

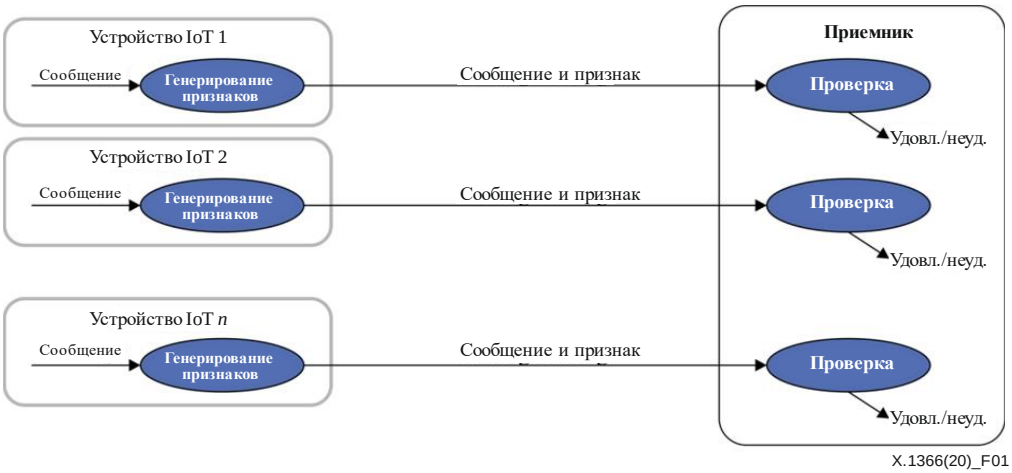

Рисунок 1 − Система прямой аутентификации (обычная система)

6.2 Базовая концепция системы совокупной аутентификации сообщений

6.2.1 Общие положения

На рисунке 2 показана базовая схема совокупной аутентификации сообщений (AMA), предлагаемая в настоящей Рекомендации. В сетевую систему IoT устанавливается узел агрегирования признаков MAC/аутентификационных признаков без изменения форматов ввода или структур существующих MAC в сети. Узел агрегирования сжимает несколько признаков MAC, прикрепленных к нескольким генерированным разными устройствами сообщениям, в один совокупный признак без ущерба для безопасности, и этот совокупный признак передается по основному каналу связи получателю для выполнения процессов проверки признака. Получатель проверяет достоверность нескольких сообщений по совокупному признаку, который позволяет выявить недействительные сообщения или данные. Этот метод эффективен для уменьшения объема передаваемых данных, когда размер совокупного признака намного меньше общего размера нескольких признаков MAC.

В настоящей Рекомендации содержится описание схемы AMA для IoT в качестве основного механизма и схемы с интерактивной AMA (IAMA) для объяснения способа выполнения процессов агрегирования и проверки. В схеме AMA для передачи совокупного признака используется только основной канал связи между узлом агрегирования и приемником. Алгоритмы агрегирования и проверки схемы AMA описаны в разделе 7. В схеме IAMA в дополнение к основному каналу используется канал обратной связи, который представляет собой аутентифицированный канал с низкой пропускной способностью между приемником и узлом агрегирования. Передавая результат проверки от приемника к узлу агрегирования по каналу обратной связи, узел агрегирования может эффективнее сжимать признаки MAC, чем AMA, описанной в разделе 7. Для проверки выполняется интерактивный протокол связи между узлом агрегирования и получателем, описанный в разделе 8.

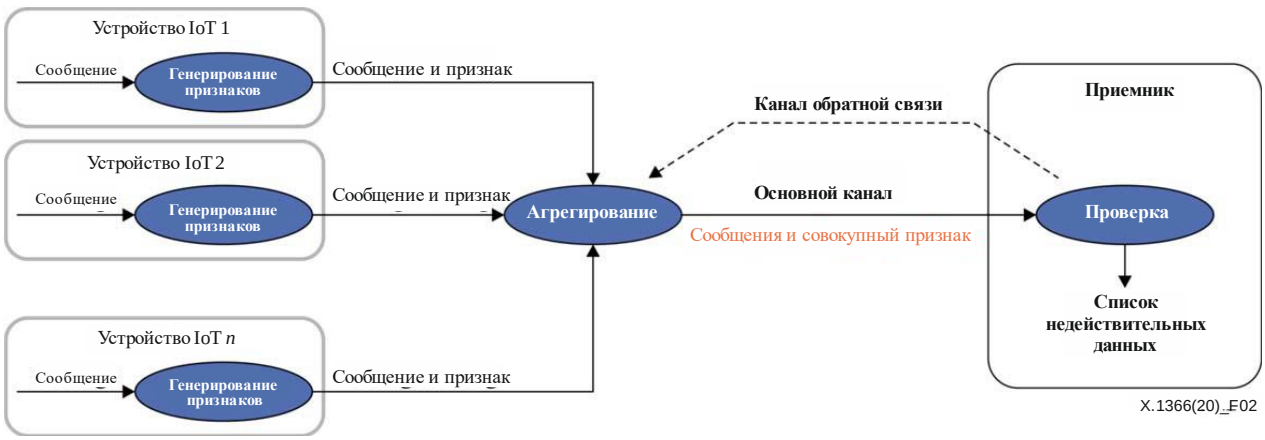

Рисунок 2 − Базовая концепция системы совокупной аутентификации сообщений

ПРИМЕЧАНИЕ. – Метод агрегирования, описанный в настоящей Рекомендации, может применяться для сжатия нескольких MAC-признаков в ситуации, когда несколько устройств передают конфиденциальные данные с использованием схем шифрование–MAC.

В настоящей Рекомендации для реализации схем AMA и IAMA используются четыре процесса – генерирование ключей, генерирование признаков, агрегирование и проверка:

1) алгоритм генерирования ключей принимает в качестве входных данных параметр безопасности и идентификатор и создает секретный ключ для этого идентификатора;

2) алгоритм генерирования признаков принимает в качестве входных данных сообщение, идентификатор и секретный ключ для этого идентификатора и выводит признак;

3) алгоритм агрегирования принимает в качестве входных данных несколько наборов идентификаторов, сообщений и признаков от нескольких устройств и на выходе создает набор совокупных признаков;

4) алгоритм проверки принимает в качестве входных данных все секретные ключи, несколько пар идентификаторов и сообщений от нескольких устройств, а также набор совокупных признаков. Он указывает недействительные сообщения и выводит список идентификаторов устройств, сообщения которых оказались недействительными.

7 Совокупная аутентификация сообщений

7.1 Общие положения

Схема AMAC, описанная в настоящей Рекомендации, обеспечивает функциональные возможности для агрегирования нескольких MAC-признаков в более короткий признак и выявления недействительных сообщений. В данном разделе объясняется, каким образом строятся четыре алгоритма – алгоритмы генерирования ключей, генерирования признаков, агрегирования и проверки – для создания AMAC.

7.2 Условные обозначения

В настоящей Рекомендации используются следующие условные обозначения:

n: количество устройств;

d: количество недействительных сообщений от устройств;

id: идентификатор устройства. ID = $\{id_1, id_2, \ldots, id_n\}$ – набор всех идентификаторов;

m: сообщение;

k_{id}: секретный ключ идентификатора id устройства. Для простоты секретный ключ, соответствующий id_i, обозначается k_i вместо k_{id_i};

$F()$: функция MAC, принимающая в качестве входных данных секретный ключ и сообщение и выводящая признак MAC;

$G = (g_{i,j})$: d-дизъюнктная матрица из u строк и n столбцов. Матрица G содержит записи вида $\{0, 1\}$, а ее столбцы индексированы идентификаторами $id_1, id_2, \ldots, id_n$. G называется d-дизъюнктной матрицей, если логическая сумма любых d столбцов матрицы G не содержит никаких других столбцов, в которых $x = (x_1, x_2, \ldots, x_u)$ *содержит* $y = (y_1, y_2, \ldots, y_u)$ при $x_i \geq y_i$ для каждого $1 \leq i \leq u$;

$I(G, i)$: множество j ($1 \leq j \leq n$), такое, что $g_{i,j} = 1$ для каждого $i = 1, 2, \ldots, u$;

$\oplus$: побитовая операция XOR (исключающее ИЛИ);

$H()$: хеш-функция.

7.3 Описание алгоритма

Для охвата более широкого спектра применений предусмотрены два вида совокупных MAC с возможностью обнаружения. Один основан на операциях XOR (пункт 7.3.1), а другой – на хеш-функции (пункт 7.3.2).

7.3.1 Конструкция на основе операции XOR

7.3.1.1 Генерирование ключей

Этот процесс генерирует для каждого идентификатора *id* случайный ключ. Он обозначается k_{id}.

7.3.1.2 Генерирование признаков

Алгоритм генерирования признаков принимает в качестве входных данных сообщение, идентификатор и секретный ключ, соответствующий идентификатору, которые обозначаются соответственно *id*, *m*, k_{id}, и выводит признак MAC *t*, вычисленный функцией *F* (k_{id}, *m*).

7.3.1.3 Агрегирование

Алгоритм агрегирования принимает в качестве входных данных идентификаторы, сообщения и их признаки MAC от *n* устройств, обозначаемые $(id_1, m_1, t_1), \ldots, (id_n, m_n, t_n)$. Для каждого i $(1 \le i \le u)$ выполняется побитовая операция XOR над признаками MAC, соответствующие идентификаторы которых содержатся в $I(G, i)$, и ее результат обозначается T_i, то есть $T_i = \oplus_{j \in I(G,i)} t_j$. Выходное значение $(T_1, T_2, \ldots, T_u)$ представляет собой совокупный признак.

7.3.1.4 Проверка

Алгоритм проверки принимает в качестве входных данных все секретные ключи (k_1, …, k_n), множество пар идентификаторов и сообщений от *n* устройств, обозначаемых $(id_1, m_1), \ldots, (id_n, m_n)$, и совокупный признак $(T_1, T_2, \ldots, T_u)$. Он выводит список J после выполнения следующей процедуры.

Шаг 1: $J \leftarrow \{id_1, id_2, \ldots, id_n\}$

Шаг 2: Для $i = 1, 2, \ldots, u$ выполнить:

если $T_i = \oplus_{j \in I(G,i)} t_j$, то $J \leftarrow J \setminus \{id_j\}$ для всех $j \in I(G, i)$.

7.3.2 Конструкция на основе хеш-функции

7.3.2.1 Генерирование ключей

Этот процесс генерирует для каждого идентификатора *id* случайный ключ. Он обозначается k_{id}.

7.3.2.2 Генерирование признаков

Алгоритм генерирования признаков принимает в качестве входных данных сообщение, идентификатор и секретный ключ, соответствующий идентификатору, которые обозначаются соответственно *id*, *m*, k_{id}, и выводит признак MAC *t*, вычисленный функцией $F(k_{id}, m)$.

7.3.2.3 Агрегирование

Алгоритм агрегирования принимает в качестве входных данных идентификаторы, сообщения и их признаки MAC от *n* устройств, обозначаемые $(id_1, m_1, t_1), \ldots, (id_n, m_n, t_n)$. Для каждого i $(1 \le i \le u)$ вычисляется хеш-значение признаков MAC, соответствующие идентификаторы которых входят в $I(G, i)$ и результат обозначается T_i, то есть $T_i = H(t_{j1}, t_{j2}, \ldots)$, где $I(G, i) = \{j_1, j_2, \ldots\}$ при $1 \le j_1 < j_2 < \ldots$.

Выходное значение (T_1, T_2, …, T_u) представляет собой совокупный признак.

7.3.2.4 Проверка

Алгоритм проверки принимает в качестве входных данных все секретные ключи (k_1, …, k_n), множество пар идентификаторов и сообщений от *n* устройств, обозначаемых (id_1, m_1), …, (id_n, m_n), и совокупный признак (T_1, T_2, …, T_u). Он выводит список J после выполнения следующей процедуры.

Шаг 1: $J \leftarrow \{id_1, id_2, \ldots, id_n\}$

Шаг 2: Для $i = 1, 2, \ldots, u$ выполнить:

если $T_i = H(t_{j_1}, t_{j_2}, \ldots)$, где $I(G, i) = \{j_1, j_2, \ldots\}$ при $1 \le j_1 < j_2 < \ldots$,
то $J \leftarrow J \setminus \{id_j\}$ для всех $j \in I(G, i)$.

8 Интерактивная совокупная аутентификация сообщений

8.1 Общие положения

Схема IAMA, предлагаемая в настоящей Рекомендации, обеспечивает функциональные возможности, позволяющие IAMA идентифицировать недействительные сообщения при меньшем размере признаков, чем в схеме AMA, описанной в разделе 7. Схема IAMA состоит из двух алгоритмов, таких как алгоритмы генерирования ключей и генерирования признаков, и интерактивного протокола связи между алгоритмами агрегирования и проверки. В данном разделе объясняется, как строятся эти алгоритмы и протокол.

8.2 Условные обозначения

В настоящей Рекомендации используются следующие условные обозначения.

n: количество устройств;

d: количество недействительных сообщений от устройств;

id : идентификатор устройства. ID = {id_1, id_2, …, id_n} – набор всех идентификаторов;

m: сообщение;

k_{id} : секретный ключ идентификатора *id* устройства. Для простоты секретный ключ, соответствующий id_i, обозначается k_i вместо k_{id_i};

F(): функция MAC, принимающая в качестве входных данных секретный ключ и сообщение и выводящая признак MAC;

AGT: протокол адаптивного группового тестирования;

⊕: побитовая операция XOR (исключающее ИЛИ);

H(): хеш-функция.

8.3 Спецификация интерактивного протокола

IAMA может состоять из функции MAC *F*() и AGT; описание адаптивного группового тестирования см. в Дополнении III. Здесь представлены такие конструкции с использованием операций двух видов – XOR или хеш-функции, – как описано в конструкциях AMA.

8.3.1 Конструкция на основе операции XOR

8.3.1.1 Генерирование ключей

Этот процесс генерирует для каждого идентификатора *id* случайный ключ. Он обозначается k_{id}.

8.3.1.2 Генерирование признаков

Алгоритм генерирования признаков принимает в качестве входных данных сообщение, идентификатор и секретный ключ, соответствующий идентификатору, которые обозначаются соответственно *id*, *m*, k_{id}, и выводит признак MAC *t*, вычисленный функцией $F(k_{id}, m)$.

8.3.1.3 Агрегирование и проверка

Агрегирование и проверка строятся на основе протокола AGT, как показано на рисунке 3. Алгоритм агрегирования принимает в качестве входных данных все множество идентификаторов ID = {id_1, id_2, …, id_n}, сообщений и их признаков MAC от *n* устройств, которые обозначаются (m_1, t_1), …, (m_n, t_n), где (m_1, t_1) ($1 \le i \le n$) – пара сообщение–признак, соответствующая id_i. Алгоритм проверки принимает все множество идентификаторов ID и все секретные ключи k_i ($1 \le i \le n$), соответствующие id_i. Сначала алгоритм агрегирования выбирает подмножество $S \subseteq$ ID, генерирует совокупный признак T_S путем сжатия признаков MAC *S*. T_S можно сгенерировать, выполнив операцию XOR над признаками MAC, $T_S = \oplus_{j \in S} t_j$. Затем алгоритм агрегирования передает T_S с сообщениями $(m_1, \ldots, m_n)$ для проверки. Процесс проверки устанавливает J = ID и проверяет достоверность T_S, используя секретные ключи *S*. T_S считается действительным, если $T_S = \oplus_{j \in S} t_j$, где $t_j = F(k_j, m_j)$; в противном случае T_S считается недействительным. Если T_S является действительным, устанавливается $J \leftarrow J \setminus S$. Процесс проверки передает результат проверки T_S (то есть один бит информации) в процесс

агрегирования. Затем алгоритм агрегирования выбирает другое подмножество $S' \subseteq ID$, генерирует совокупный признак $T_{S'}$ путем сжатия признаков MAC S' и передает $T_{S'}$ для проверки. Алгоритм проверки проверяет достоверность $T_{S'}$, используя секретные ключи S'; если $T_{S'}$ является действительным, $J \leftarrow J \setminus S'$. Алгоритм проверки передает результат проверки $T_{S'}$ в процесс агрегирования. После повторения описанных выше процедур между процессами агрегирования и проверки последний выводит окончательный список J, состоящий из идентификаторов устройств, сообщения которых оказались недействительными.

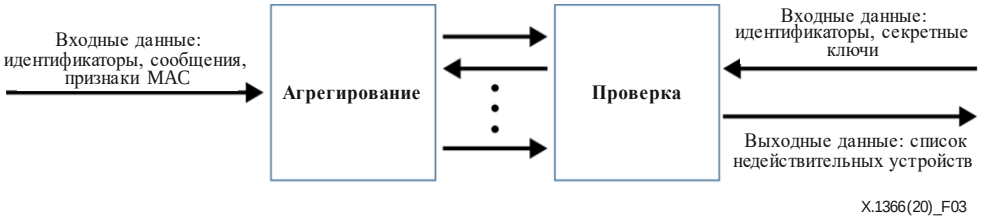

Рисунок 3 − Интерактивный протокол между процессами агрегирования и проверки

8.3.2 Конструкция на основе хеш-функции

8.3.2.1 Генерирование ключей

Этот процесс генерирует для каждого идентификатора *id* случайный ключ. Он обозначается k_{id}.

8.3.2.2 Генерирование признаков

Алгоритм генерирования признаков принимает в качестве входных данных сообщение, идентификатор и секретный ключ, соответствующий идентификатору, которые обозначаются соответственно *id*, *m*, k_{id}, и выводит признак MAC *t*, вычисленный функцией $F(k_{id}, m)$.

8.3.2.3 Агрегирование и проверка

Агрегирование и проверка строятся на основе протокола AGT, как показано на рисунке 3. Алгоритм агрегирования принимает в качестве входных данных все множество идентификаторов $ID = \{id_1, id_2, \ldots, id_n\}$ сообщений и их признаков MAC от n устройств, которые обозначаются $(m_1, t_1), \ldots, (m_n, t_n)$, где (m_i, t_i) $(1 \leq i \leq n)$ – пара сообщение–признак, соответствующая id_i. Алгоритм проверки принимает все множество идентификаторов *ID* и все секретные ключи k_i $(1 \leq i \leq n)$, соответствующие id_i. Сначала алгоритм агрегирования выбирает подмножество $S \subseteq ID$ генерирует совокупный признак T_S путем вычисления хеш-значения $T_s = H(tj_1, tj_2, (\ldots))$, где $S = \{id_{j1}, id_{j2}, \ldots\}$ при $1 \leq j_1 < j_2 < \ldots$. Затем алгоритм агрегирования передает T_S с сообщениями $(m_1, \ldots, m_n)$ для проверки. Процесс проверки устанавливает $J = ID$ и проверяет достоверность T_S, используя секретные ключи *S*. T_S считается действительным, если $T_s = H(tj_1, tj_2, \ldots)$, где $t_j = F(k_j, m_j)$; в противном случае T_S считается недействительным. Если T_S является действительным, устанавливается $J \leftarrow J \setminus S$. Процесс проверки передает результат проверки T_S (то есть один бит информации) в процесс агрегирования. Затем алгоритм агрегирования выбирает другое подмножество $S' \subseteq ID$, генерирует совокупный признак $T_{S'}$ путем сжатия признаков MAC S' и передает $T_{S'}$ для проверки. Алгоритм проверки проверяет достоверность $T_{S'}$, используя секретные ключи S'; если $T_{S'}$ является действительным, $J \leftarrow J \setminus S'$. Алгоритм проверки передает результат проверки $T_{S'}$ в процесс агрегирования. После повторения описанных выше процедур между процессами агрегирования и проверки последний выводит окончательный список *J*, состоящий из идентификаторов устройств, сообщения которых оказались недействительными.

Приложение A

Руководящие указания и ограничения

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

A.1 Руководящие указания по использованию совокупной аутентификации сообщений (AMA)

В настоящей Рекомендации обсуждается применимость встраивания узла агрегирования в существующие протоколы кода аутентификации сообщений (MAC) без изменения форматов входных данных или сетевых соединений базовых MAC. Кроме того, агрегирование – это процедура без ключей, не требующая обслуживания какого-либо секретного ключа в узле агрегирования. Причем агрегирование выполняется только путем вычисления побитовых операций XOR или хеш-функций, и, следовательно, для упрощенной аутентификации подходят схемы AMA, описанные в настоящей Рекомендации.

При обработке, связанной с агрегированием и описанной в разделе 7, необходимо сгенерировать и сохранить d-дизъюнктную матрицу. Известно несколько методов генерирования d-дизъюнктных матриц, таких как описанные в [b-TM05], и можно также использовать сжатую форму d-дизъюнктной матрицы, описанную в [b-MK19]. В настоящей Рекомендации предлагается использовать эти методы даже в схемах AMA. Для d-дизъюнктной матрицы из u строк и n столбцов схема AMA эффективнее, чем традиционная прямая аутентификация, если $u < n$, и еще эффективнее, если $d \ll \sqrt{n}$.

ПРИМЕЧАНИЕ. – Уровни безопасности описанных здесь схем AMA (или IAMA), построенных на основе побитовой операции XOR или хеш-функций, соответствуют уровням безопасности схем, описанных в [b-HS18] и [b-SS19]. Имеется три вида понятий безопасности: невозможность подделки (unforgeability), полнота идентифицируемости (identifiability-completeness) и нестрогая надежность идентифицируемости (identifiability-(weak)-soundness). Невозможность подделки гарантирует, что никакое сообщение не может быть подделано. Полнота идентифицируемости гарантирует, что любое действительное сообщение будет признано схемой как действительное. Надежность идентифицируемости гарантирует, что любое недействительное сообщение будет признано схемой как недействительное, а нестрогая надежность идентифицируемости – это то же, что и надежность идентифицируемости, за исключением того, что злоумышленник предположительно не получает действительных MAC-признаков и не повреждает никаких устройств перед атакой. Нестрогая надежность все же полезна в конкретных применениях, поскольку она охватывает подделку сообщений.

Уровни безопасности схем AMA (или IAMA), описанных в настоящей Рекомендации, интерпретируются следующим образом. Конструкция, основанная на операции XOR, отвечает требованиям невозможности подделки, полноты идентифицируемости и нестрогой надежности идентифицируемости, если базовый MAC отвечает требованию невозможности подделки. Конструкция, основанная на хеш-функции, отвечает требованиям невозможности подделки, полноты идентифицируемости и надежности идентифицируемости, если базовый MAC отвечает требованию невозможности подделки, а хеш-функция представляет собой случайную функцию.

A.2 Ограничения использования AMA

В настоящей Рекомендации предполагается, что число недействительных сообщений в схемах AMA не превышает d, и этот параметр устанавливается как системный. Это означает, что необходимо предварительно вычислить возможное число d.

Что произойдет, если количество недействительных сообщений превысит предполагаемое значение d? В этом случае на выходе операции проверки будет выведен список J, содержащий больше чем d идентификаторов устройств. Идентификаторы устройств, отправивших недействительные сообщения, включены в список J; однако в список J также могут попасть и некоторые идентификаторы устройств, не отправлявших недействительных сообщений. В этом случае рекомендуется увеличить значение d для схемы AMA.

Приложение B

Сочетание с существующими протоколами прямой аутентификации

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

Схемы AMA (или IAMA), описанные в настоящей Рекомендации, могут использоваться в сочетании с традиционной прямой аутентификацией. Под традиционной прямой аутентификацией понимается схема AMA, в которой базовая дизъюнктная матрица представляет собой единичную матрицу. Для $n = n_1 + n_2$ устройств, если предпочтительно агрегировать только n_1 из n MAC-признаков, выполняются следующие действия: к n_1 устройствам применяется схема AMA (или IAMA), а в отношении остальных n_2 устройств выполняется прямая аутентификация, как показано на рисунке B.1.

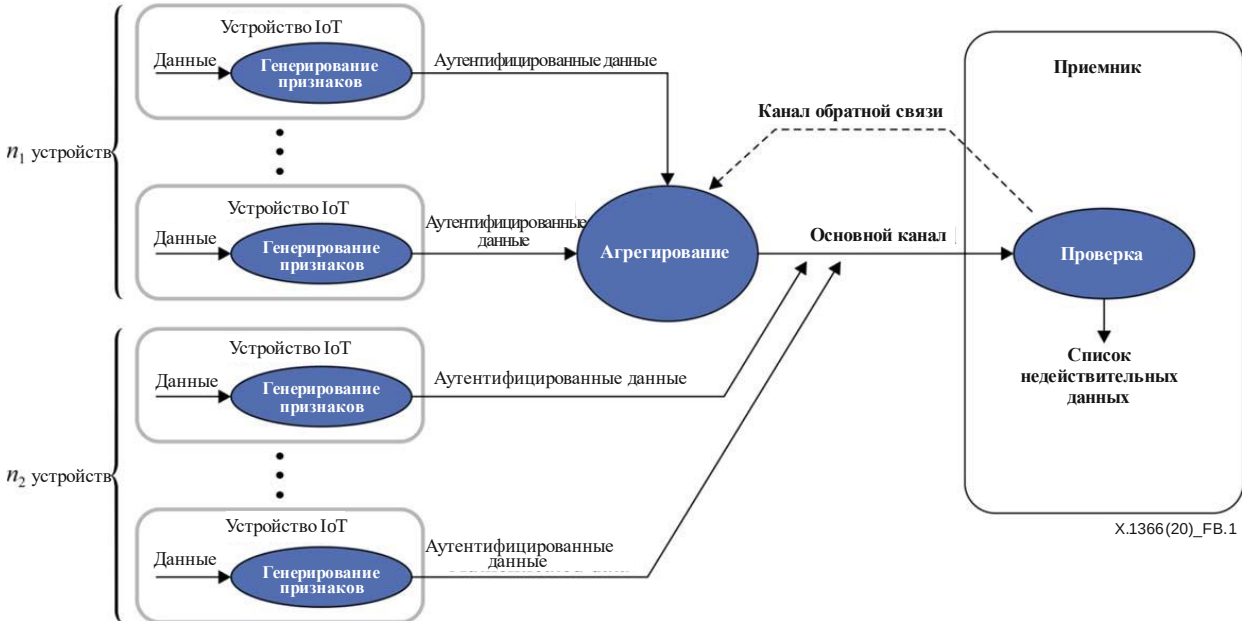

Рисунок B.1 − Сочетание с протоколами прямой аутентификации

Дополнение I

Сценарии использования AMA

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

I.1 Введение

Схема совокупной аутентификации сообщений может применяться для обеспечения аутентификации объекта (личности), а также аутентификации сообщений. Кроме того, эта схема, возможно, применима не во всех сценариях использования устройств интернета вещей (IoT). В частности, данная схема достаточно эффективна и подходит для использования при следующих условиях:

- требуется аутентификация сообщений от десятков до десятков тысяч устройств IoT;
- данные/сообщения, обрабатываемые в процессе аутентификации, поступают часто и нерегулярно.

Ниже приведены примеры приложений, в которых, как можно определенно предположить, будет использоваться технология совокупной аутентификации:

a) приложения для частой отправки сжатых данных/сообщений, таких как короткометражные видеофильмы (фотографии):
   - приложения видеонаблюдения;

b) приложения для дистанционной телеметрии:
   - приложения наблюдения за работой завода;
   - приложения для исследования динамики аудитории;
   - приложения для наблюдения за состоянием здоровья, например во время городского марафона;
   - приложения для управления такими объектами, как уличные фонари в городских районах;
   - приложения для регулирования дорожного движения;
   - приложения для мониторинга уровня рек.

Применение данной технологии совокупной аутентификации в вышеупомянутых приложениях IoT может существенно повысить эффективность процессов передачи сообщений и аутентификации в системе IoT в целом.

Ниже приведены сценарии использования схемы совокупной аутентификации, описанной в настоящей Рекомендации.

I.2 Сценарий использования 1. Тематические парки и развлекательные центры

Можно предположить, что в случае парков и развлекательных центров число одновременно посещающих их людей составляет от 1000 до 10 000 человек. То есть может потребоваться одновременная аутентификация тысяч посетителей, имеющих соответствующие права на использование аттракционов в парке/развлекательном центре. В этом случае схема совокупной аутентификации может идеально подойти для эффективного управления авторизацией. Как показано на рисунке I.1, в каждом аттракционе могут находиться серверы агрегирования для сбора и агрегирования аутентификационных признаков в целях запроса проверки у центрального сервера аутентификации.

В частности, посетители заранее покупают входные билеты, в которых на встроенном микрочипе указана информация о посещении мероприятий, аттракционов и о предоставляемых веб-услугах. Эта технология широко применяется при марафонах. В качестве альтернативы входным билетам также можно использовать браслеты со встроенными чипами.

У главных ворот места проведения мероприятия или у отдельного входа в каждый аттракцион содержимое входного билета считывается, агрегируется с использованием технологии совокупной аутентификации и передается на сервер совокупной аутентификации.

Серверный центр совокупной аутентификации анализирует содержание и требования к услугам, предоставляемым посетителям, информирует различные аттракционы и поставщиков веб-услуг, а также использует их для анализа и прогнозирования загрузки. После проверки посетители могут пользоваться различными зарегистрированными веб-услугами, например через свои смартфоны или носимые устройства типа очков.

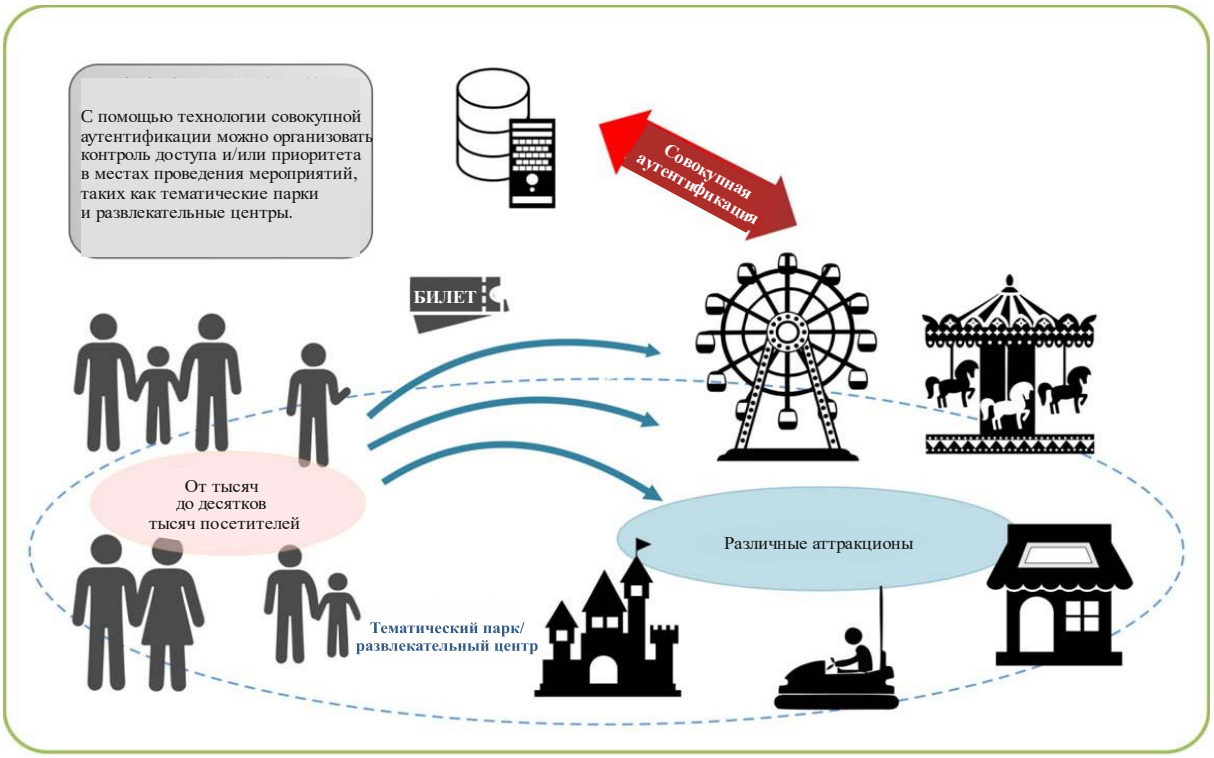

Рисунок I.1 − Схема совокупной аутентификации в тематических парках и развлекательных центрах

I.3 Сценарий использования 2. Датчики видеонаблюдения

I.3.1 Общие положения

Одним из сценариев использования схем совокупной аутентификации, представленных в настоящей Рекомендации, может служить мониторинг обстановки с использованием датчиков наблюдения, таких как камеры устройств IoT, для получения оповещений и возможности вмешаться на ранней стадии в случае стихийных бедствий или аварий/инцидентов. В этом случае квази-видеозаписи или неподвижные изображения с нескольких камер наблюдения передаются в центр наблюдения практически в режиме реального времени (или периодически), но важно обеспечить надежность и целостность передаваемых данных.

Однако когда количество датчиков наблюдения становится очень большим, уже неэффективно последовательно проверять коды аутентификации данных изображения с каждой камеры. В этом случае полезна схема совокупной аутентификации. Перед отправкой в центр наблюдения коды аутентификации данных можно объединить на серверах агрегирования, с тем чтобы система IoT в целом могла обеспечить эффективную аутентификацию и связь. Количество серверов агрегирования зависит от количества датчиков наблюдения. На рисунке I.2 показаны датчики наблюдения в схеме совокупной аутентификации.

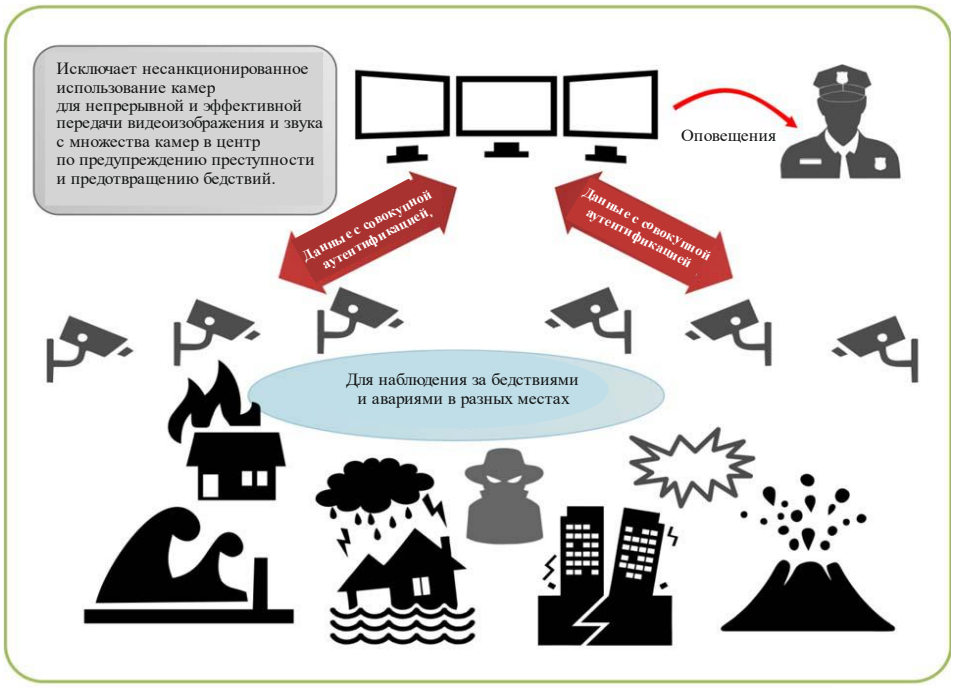

Рисунок I.2 − Датчики наблюдения в схеме совокупной аутентификации

I.3.2 Конкретные сценарии использования

1) Контроль среды проживания, такой как населенные пункты и жилые дома

Информация о среде проживания, поступающая от различных датчиков, таких как камеры видеонаблюдения, установленные в многоквартирных домах, "умных" населенных пунктах, частных домах и т. д., собирается в шлюзе (концентратор IoT) и передается на центральный сервер с использованием технологии совокупной аутентификации.

Центр анализирует полученную информацию и использует ее для контроля среды проживания, прогнозирования аномалий и отказов, быстрого реагирования и предотвращения преступлений и бедствий.

Более конкретно, данные, поступающие от различных датчиков состояния окружающей среды, датчиков бытовой техники, камер наблюдения, датчиков открытия/закрытия дверей/окон, датчиков состояния инфраструктуры газо/водо/электроснабжения, датчиков контроля лифтов и т. д., передаются во внешние центры. Схемы совокупной аутентификации, использующие как аутентификацию терминалов, так и аутентификацию данных, полезны в качестве средства аутентификации для сбора больших объемов разнообразных данных и эффективной передачи данных.

2) Обслуживание и контроль социальной инфраструктуры, реагирование на бедствия

В настоящее время в различных областях внедряется техническое обслуживание объектов социальной инфраструктуры, таких как мосты, туннели и дороги, и управление ими с использованием IoT, и ожидается, что в ближайшем будущем услуги IoT станут играть чрезвычайно важную роль в создании безопасного и защищенного общества. Так в случае старения мостов и эстакад различные датчики детально регистрируют соответствующие данные, такие как сведения о деформации, вибрации, смещении, наклоне и т. д., а также видеоинформацию. Объем данных, которые необходимо передавать в центр, становится чрезвычайно большим.

В настоящее время метод совокупной аутентификации оказывается чрезвычайно эффективным в качестве одной из мер повышения эффективности использования беспроводной сети интернет и для предотвращения перегрузки. В дополнение к обслуживанию объектов социальной инфраструктуры и управлению ими метод совокупной аутентификации также можно применить к шлюзу системы IoT для использования систем постоянного мониторинга изменения уровня воды и стока рек и озер в сельскохозяйственной среде.

3) Системы предотвращения бедствий с использованием камер наблюдения

Камеры наблюдения установлены в разных местах по всему миру и используются для различных целей, включая предупреждение преступности и предотвращение бедствий. Как правило, в сети, обрабатывающей видео- и аудиоинформацию, необходимо непрерывно передавать на центральную станцию большие объемы данных, и метод совокупной аутентификации хорошо подходит для их эффективной передачи. Он позволяет повысить эффективность связи между устройством IoT и шлюзом IoT, а также между шлюзом IoT и центральной станцией.

4) Логистический мониторинг, повышение эффективности транспортных систем

В логистике и транспортных бизнес-системах системы IoT все чаще используются для повышения эффективности и расширения функциональных возможностей предприятий. Например находит широкое практическое применение решение, позволяющее точно управлять информацией о состоянии товаров и упаковок от отгрузки до доставки. В такой системе, применяя технологии совокупной аутентификации к системе, передающей в центр информацию от различных датчиков обо всех упаковках, можно добиться более стабильного и эффективного управления логистикой. Можно также создать шлюз IoT для транспортных средств, таких как автомобили, оснащенные огромным количеством датчиков, и применять технологию совокупной аутентификации на уровне шлюза транспортных средств в транспортных системах.

Дополнение II

Соответствующая деятельность по схемам AMA

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Схема AMA, которая отличается от схемы, описанной в разделе 7, и позволяет объединить несколько признаков MAC нескольких сообщений в более короткий признак, была впервые предложена Кацем и Линделлом в [b-KL08]. В частности, Кац и Линделл в [b-KL08] формально описали модель и безопасность AMA и представили простую конструкцию AMA, выполняющую побитовую операцию XOR над всеми признаками MAC. В предложенной ими схеме AMA можно проверить достоверность нескольких сообщений с укороченным одиночным признаком, однако если несколько сообщений признаны недействительными по отношению к одному признаку, то выявить недействительные сообщения, как правило, невозможно. Схемы AMA, описанные в настоящей Рекомендации, обеспечивают как функциональные возможности объединения нескольких MAC-признаков в более короткий признак, так и выявление недействительных сообщений. Код AMA, представленный в разделе 7 настоящей Рекомендации, основан на [b-HS18], тогда как интерактивный протокол аутентификации для использования AMA, представленный в разделе 8, основан на [b-SS19].

Дополнение III

Протокол адаптивного группового тестирования

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Групповое тестирование, которое рассматривается в [b-DH00], представляет собой метод определения особых элементов, называемых дефектными, среди большого количества полноценных элементов с использованием небольшого числа тестов вместо проведения тестирования каждого элемента по отдельности.

В следующем примере протокола группового тестирования, который показан на рисунке III.1, предполагается, что имеется n элементов, d из которых являются дефектным.

При адаптивном групповом тестировании тесты могут проводиться несколько раз, так что поднабор тестируемых элементов можно выбрать после получения результатов предыдущего теста. Конкурентное групповое тестирование – это адаптивное групповое тестирование, для которого не требуется знать заранее количество дефектных элементов d.

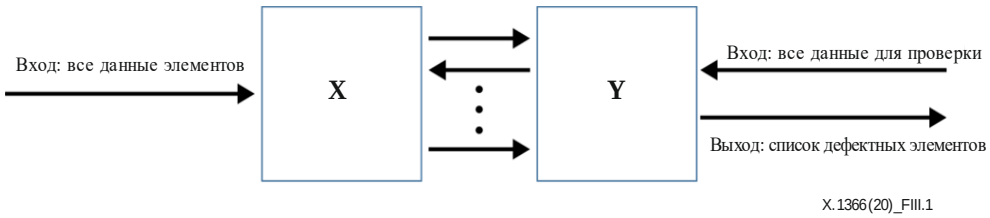

Рисунок III.1 − Протокол адаптивного группового тестирования

Формально адаптивное групповое тестирование – это интерактивный протокол обмена данными между X и Y, как показано на рисунке III.1.

X принимает все множество идентификаторов $ID = \{id_1, id_2, \ldots, id_n\}$ и все данные элементов data_i $(1 \leq i \leq n)$, соответствующие id_i. Y принимает все множество идентификаторов ID и все данные проверки ans_i $(1 \leq i \leq n)$, соответствующие id_i. Сначала X выбирает подмножество $S \subseteq ID$, генерирует test_S путем сжатия данных элементов S и передает test_S в Y. Затем Y устанавливает $J = ID$ и проверяет действительность test_S, используя данные проверки S. Если test_S является действительным, устанавливается $J \leftarrow J \setminus S$. Y передает результат проверки test_S (то есть один бит информации) в X. Затем X выбирает другое подмножество идентификаторов и повторяет процедуры между X и Y. После повторения вышеуказанных процедур между X и Y, Y выводит окончательный список J, состоящий из идентификаторов дефектов.

Например к протоколам адаптивного группового тестирования относятся двоичный поиск, алгоритм прочесывания и отсеивания (rake-and-winnow algorithm) [b-EGH07], многоэтапный алгоритм Ли [b-Li62] и алгоритм вычерпывания (digging algorithm), описанный в пункте 4.6 [b-DH00].

Библиография

[b-ITU-T X.813] Recommendation ITU-T X.813 (1996), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Non-repudiation framework*.

[b-DH00] D. Z. Du and F. K. Hwang, *Combinatorial Group Testing and Its Applications*, Series on Applied Mathematics, vol. 12, 2nd edn. World Scientific, Singapore, 2000.

[b-EGH07] D. Eppstein, M. T. Goodrich, and D. S. Hirschberg, *Improved Combinatorial Group Testing Algorithms for Real-world Problem Sizes*, SIAM J. Comput. 36(5), pp. 1360−1375, 2007.

[b-HS18] S. Hirose and J. Shikata, *Non-adaptive Group-Testing Aggregate MAC Schemes*, The 14th International Conference on Information Security Practice and Experience (ISPEC 2018), LNCS 11125, pp. 357-372, Springer, 2018.

[b-KL08] J. Katz and A.Y. Lindell, *Aggregate message authentication codes*, CT-RSA 2008, LNCS 4964, pp. 155-169. Springer, 2008.

[b-Li62] C. H. Li, *A Sequential Method for Screening Experimental Variables*, J. Am. Stat. Assoc. 57 (298), pp. 455-477, 1962.

[b-MK19] K. Minematsu and N. Kamiya, *Symmetric-key Corruption Detection: When XOR-MACs meet combinatorial group testing*, ESORICS 2019, Part I, LNCS 11735, pp. 595-615, Springer, 2019.

[b-MOV96] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, October 1996, Fifth Printing (August 2001).

[b-SS19] S. Sato and J. Shikata, *Interactive Aggregate Message Authentication Scheme with Detecting Functionality*, The 33rd International Conference on Advanced Information Networking and Applications (AINA-2019), pp. 1316-1328, Springer, 2019.

[b-TM05] N. Thierry-Mieg, *A New Pooling Strategy for High-throughput Screening: the Shifted Transversal Design*, *BMC Bioinformatics*, vol. 7, no. 28, 2005.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация, а также соответствующие измерения и испытания
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2021 г.