УДК 681.325

В.Я. Певнев[1], В.В. Торяник[1], Е.В. Торяник[2], Г.З. Халимов[2]

[1]*Харьковский национальный университет внутренних дел, Харьков*
[2]*Харьковский национальный университет радиоэлектроники, Харьков*

ПРОТОКОЛЫ МНОГОАДРЕСНОЙ АУТЕНТИФИКАЦИЯ С ОБЕСПЕЧЕНИЕМ НЕОТРЕКАЕМОСТИ, ДОПУСКАЮЩИЕ ПОТЕРЮ ПАКЕТОВ

Рассмотрены протоколы многоадресной аутентификации при наличии помех в каналах связи, приводящих к потери пакетов. Представленные протоколы позволяют идентифицировать автора сообщения и гарантировать его неотрекаемость.

Ключевые слова: *аутентификация, пакет, протокол, хеш-функция.*

Введение

Согласно Конституции Украины [1] обеспечение информационной безопасности (ИБ) относится к наиболее важным функциям государства. Это положение показывает место ИБ в безопасности всего государства. В качестве стандартной модели безопасности часто приводят модель CIA (конфиденциальность, целостность, доступность) [2]. Когда говорят о целостности сообщения, интуитивно возникает вопрос об авторстве полученной информации. Поэтому одним из базовых вопросов информационной безопасности является аутентификация. Аутентификация многоадресных источников в реальном времени является нетривиальной криптографической задачей и активно исследуется.

В протоколах, которые гарантируют аутентификацию источника данных и неотрекаемость, отправитель должен подписывать сообщение, используя свой личный ключ. Простым решением является подписание каждого многоадресного сообщения и последующая групповая передача его одновременно с его подписью. При получении сообщения и его подписи, пользователи будут способны проверять подлинность источника данных сообщения, используя открытый (публичный) ключ отправителя и, таким образом, гарантируется неотрекаемость. При использовании схемы с возможной потерей пакетов необходимо, чтобы каждый пакетов нѐс аутентификационную информацию (АИ) других пакетов. В этом случае эффект единственной подписи распространяется на все взаимоотношения пакетов. Это распространение гарантирует аутентификацию источника данных и неотказуемость всех взаимосвязанных пакетов.

Целью предложенной работы является анализ существующих протоколов многоадресной аутентификация, в которых при передаче возможна потеря пакетов.

Схемы, допускающие потерю пакетов

Большинство медиапотоковых приложений не используют надѐжного транспортного уровня, так как им требуется передача в реальном времени и, следовательно, повторная передача пакетов не может использоваться для восстановления потерянных данных. Главная идея, использующаяся для борьбы с потерей пакетов в этой категории схем аутентификации источника данных, есть создание избыточности в этой АИ так, что даже если некоторые пакеты будут потеряны, то требуемая АИ будет восстановлена из полученных пакетов. Другими словами, вместо того, чтобы встраивать хеш-функцию (ХФ) пакета (ХФП) только в следующий (или предыдущий) пакет, ХФП встраивается в несколько пакетов. Это встраивание ХФП в другие пакеты для создания избыточной АИ формирует топологию взаимосвязи пакетов. При подобном подходе необходимо решить двухкритериальную задачу: одним критерием является минимизация избыточности, вторым – максимизация устойчивости к потери пакетов.

Терминология. Если пакет C_j содержит ХФП C_i ,то хеш-ссылка (ХС), соединяющая C_i с C_j и C_j , называется целевым пакетом C_i. Степень избыточности - число раз, которое ХФП включается в последующие пакеты для создания избыточности в сцеплении пакета с пакетом подписи. Пакет подписи – это последовательность ХФП, которая подписана, используя общеизвестную цифровую подпись. Точки ХС из пакета C_k к пакету подписи S_l, если S_l содержит C_k. Предполагается, что некоторые пакеты могут быть потеряны между отправителем и получателем. Доказано, что пакет C_i является проверяемым, если существует путь (следующие ХС) из C_i к пакету подписи S_j. Степенью (коэффициентом) верификации обозначается отношение числа проверенных пакетов к числу полученных пакетов. Коэффициент верификации является хорошим показателем вероятности проверки, которая означает вероятность быть проверенным при его получении: P (па-

кет проверен/пакет получен).

EMSS: Эффективная многоцепочечная подпись потока. В [3] предложена идея избыточности хэш сцепления, которая означает, что каждый пакет потока ХФ ссылается на несколько целевых пакетов. Таким образом, даже если некоторые пакеты потеряны, то полученные пакеты можно проверить, если сохранился путь ХС, который связывает пакет с пакетом подписи. Для данного пакета EMSS выбирает целевой пакет случайно. Следовательно, EMSS обеспечивает более или мене вероятностную гарантию, что существует путь ХС между пакетом и пакетом подписи для данной конкретной величины потери пакетов в сети.

EMSS работает следующим образом. Когда пакет представляется для отправки, отправитель включает некоторые ХФ других пакетов в этот пакет и вычисляет весь хэш код. Этот хэш-код буферизируется, чтобы позже включить его в d целевых пакетов, выбранных случайно отправителем (где d – степень избыточности). На рис. 1 показан пример, где степень избыточности равняется 3. В этом примере пакеты i+j, i+b, i+k – целевые пакеты пакета i. Если мы предположим, что потерянные пакеты удалены из графа, то пакет i является проверяемым, потому что он содержит путь ХС к пакету подписи S через пакет i+b.

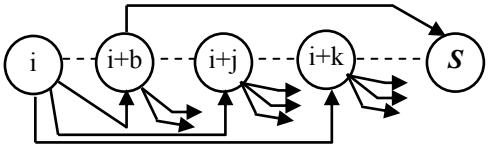

Рис. 1. EMSS хэш сцепления с уровнем избыточности равным 3

Чтобы отправителю на протяжении длительного времени гарантировать аутентификацию потока, он периодически посылает пакеты подписи. Для того, чтобы проверить подлинность полученных пакетов, отправитель буферизирует полученные пакеты и ждѐт для него соответствующего пакета подписи. Пакет подписи содержит в себе ХФП, которые позволяют проверять некоторые пакеты. Эти последние(недавние) пакеты несут в себе, в свою очередь, ХФП, которые позволяют проверять другие пакеты, и т.д. до тех пор, пока не будет проверена подлинность всех полученных пакетов.

EMSS обеспечивает вероятностную устойчивость к потере пакетов. Используя моделирование, авторы показали, что, используя показатель (коэффициент) избыточности равный 6, более, чем 90% полученных пакетов можно проверить (сохраняется путь ХС к пакету подписи), даже, если 60% пакетов потока потеряны. Главным недостатком этой схемы есть то, что получатели испытывают задержки перед проверкой полученных пакетов, так как они должны ждать пакет подписи, соответствующий полученным пакетам. Кроме того, периодическое подписывание делает это решение неприемлемым для большинства ресурсоограниченных устройств.

Дальнейшим развитием данного способа является протокол A^2Cast: протокол адаптивной аутентификации источника для многоадресных потоков [4]. A^2Cast основывается на EMSS, с тем добавлением, что у получателей существует возможность передавать отправителю коэффициент потерь в сети. Основываясь на обратной связи получателей, источник выбирает самый лучший показатель избыточности, чтобы учитывать реальный показатель потери пакетов в сети. Таким образом, A^2Cast делает возможным не только уменьшения ненужных расходов на АИ, но, также позволяет достигнуть самой лучшей величины аутентификационной проверки полученных пакетов.

p-случайная схема аутентификации. В [5] предложена избыточная и случайная схема сцепления хэшей, допускающая потерю пакетов в сети, где каждый пакет теряется независимо друг от друга с вероятностью q. Перед тем, как будет послан первый пакет потока, конструируется хэш-ссылочная топология. Случайная избыточная топология, предложенная авторами, называется p-случайным графом. В основной схеме на p-случайном графе пакеты потока нумеруются от 1 до n. C_1 – пакет подписи, а для всех пар пакетов (C_i,C_j), где i<j, ХФП C_i вставляется в пакет C_j с вероятностью p.

Сконструировав единожды p-случайный граф потока, пакеты потока передаются следующим образом. Получатель начинает прием с получения пакета. Если он правильный, то получатель проверяет последующие пакеты на лету, проверяя существование пути ХС между полученным пакетом и пакетом подписи. На рис. 2 показан простой p-случайный граф.

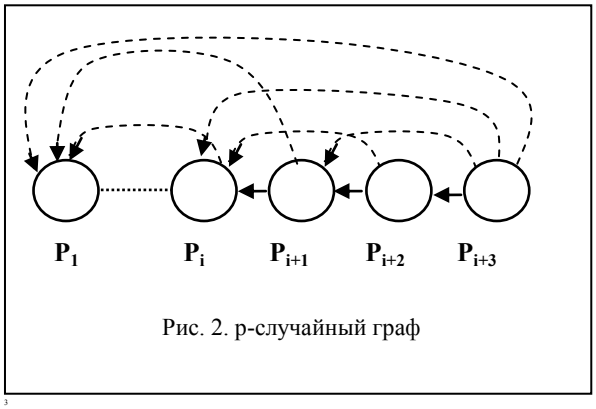

Рис. 2. p-случайный граф

В [5] показано, что с p-случайной аутентификационной схемой в сети, где каждый пакет теряется независимо случайно с вероятностью q, вероятность аутентификации каждого пакета P_i, $i \geq 2$ имеет нижнюю границу:

$P_r [P_{i\,пр} / P_{i\,пол}] \geq 1 - ((1-p)(1-(1-q))^{2})^{i-2}$.

Нижняя граница вероятности аутентификации зависит от положения пакета ι в потоке C_i, таким образом, что эта оценка является большей для пакетов, которые находятся дальше от пакета подписи. Чтобы обеспечить такой же минимум для всех пакетов, конструкция p-случайного графа была расширена добавлением большей избыточности, используя MAC, чтобы увеличить эффективное расстояние предыдущих пакетов от подписи. Получатели проверяют полученные пакеты немедленно, однако отправителю необходимо буферизировать весь поток, чтобы построить p-случайный граф потока. Расходы на АИ могут быть высокими, завися от параметра p. Более того, каждый пакет имеет среднюю ожидаемую величину избыточности, равную p(n – 1) ХС (в основных p-случайных графах).

Подход периодического сцепления. Возможны варианты построения схем, когда целевые пакеты данного пакета выбираются детерминировано, а не случайно [6]. Предложенная детерминированная топология отношения пакетов разработана таким образом, чтобы оптимизировать сопротивляемость импульсным потерям. Действительно, в Интернете последовательные пакеты имеют тенденцию быть потерянными вместе в импульсе. Целью предлагаемого подхода есть построение таких аутентификационных схем, которые могли бы противостоять импульсу максимального размера. Чтобы построить топологию ХС между пакетами, отправителю необходимо буферизировать некоторые пакеты, чтобы создать ХС между ними. Классификация предложенных топологий основывается на размерах буфера отправителя.

При отсутствии буферизации предлагается топология, называемая C_a. Она представляет собой периодическую схему аутентификации с периодом 1 и определяется следующим образом: целевыми пакетами пакета C_i есть C_{i+1} и C_{i+a}. Последний пакет C_n подписывается. C_a называется цепочкой мощности a.

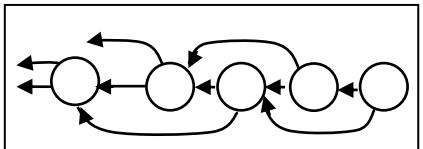

Рис. 3. Периодическая цепочка мощности 2

На рис. 3 представлен пример C_2 схемы аутентификации.

При размере буфера больше 1 предлагается топология, называемую C_a расширенной цепочкой, обозначаемую как $C_{a,p}$. $C_{a,p}$ топология основывается на C_a топологии путѐм вставки p – 2 пакетов рекурсивно между двумя пакетами C_a топологии, как показано в следующем примере. На рис. 4 показана $C_{3,6}$ топология. Пакеты A и B соответствуют пакетам, сцепленным в соответствии с C_a топологии. Затем пакеты 1 и 2 вставляются, как показано на рис. 4, а. Наконец, пакеты 3 и 4 вставляются между пакетами 1 и 2 таким же самым образом они позже они вставляются между A и B (рис. 4, б). Чтобы обеспечить долговременную аутентификацию источника данных потока, предложенная схема применяется к каждому блоку из n пакетов.

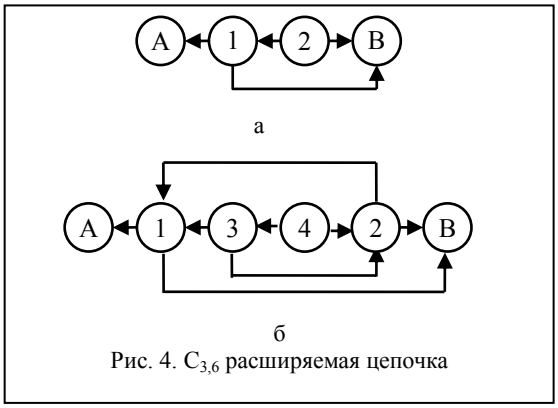

Рис. 4. $C_{3,6}$ расширяемая цепочка

С C_a схемой импульсы длиной до (a – 1) не разъединяют любой пакет с подписью. Авторы доказали, что схема C_a оптимально противостоит импульсным потерям среди всех схем, которые могут выполняться отправителем, который буферизирует один пакет и имеет хэш буфер размера a. АИ также уменьшается до двух ХФ на пакет. С C_a схемой максимальное число ХФ, добавляемых к любому пакету, является константой (пять в максимальном случае), а среднее число ХФ, добавляемых к пакету, равняется двум. Доказано, что любой импульс длины не более C_a (a – 1) пакетов оставляет поток проверяемым. Однако, число потерянных импульсов, которые могут произойти во время передачи блока вероятнее более существенно, чем одиночного импульса. Предложенное решение не оптимизировано для этих ситуаций. Действительно, с этой топологией, отправителю требуется буферизировать C пакетов перед их отправлением. Таким образом, эта топология может быть не пригодна для некоторых приложений, которые требуют широковещания в реальном времени.

Комбинирование (передача прямых и обратных пакетов). В [5] предложена схема аутентификации, основанная на технике сцепления ХФП, разработанную так, чтобы противостоять множественным импульсам. Эта схема имеет дело со сценарием, в котором данные переносятся разными пакетами, имеющие большую или меньшую важность с точки зрения уровня приложения. Пакеты объединяются в классы с разными приоритетами. Затем хэш-сцепление делается таким образом, что более высо-

кие приоритетные классы являются более устойчивыми, хэш-сцепление пакетов принадлежат к этому классу, чтобы обеспечить более высокое противодействие импульсным потерям.

В этой схеме пакеты разделяются на приоритетные классы $S_0, \dots, S_y$. Первый пакет потока и те пакеты, для которых отправитель требует высокое противодействие, помещаются в S_0 (самый высокий приоритетный класс), пакеты со следующим высоким уровнем противодействия идут в S_1 (следующий высокоприоритетный класс) и т.д. Предполагается, что пакеты в самом высоком приоритетном классе расположены с равными интервалами по всему потоку, чтобы минимизировать их вероятность быть одновременно потерянными в импульсе. Топология ХС структурирован таким образом, что узлы в S_0 допускают самые высокие импульсные потери и не требуют получения никаких узлов из низкоприоритетных классов. Затем ХС, которые берут начало в самых низких приоритетных пакетах и всегда заканчиваются в пакете в S_0, добавляются к топологии. Это означает, что ХФ низкоприоритетных пакетов помещаются только в пакеты высокоприоритетного класса.

В предложенной схеме каждый приоритетный класс S_i ассоциируется с его двумя параметрами b_i и x_i: b_i означает максимальный размер импульсов, которые должны допускать пакеты в классе, а x_i обозначает максимальное число импульсов, которые должны допускать пакеты в классе. Эта схема достаточно привлекательная, когда отправитель хочет иметь значительный контроль над потерей каждого пакета. Еѐ главным недостатком есть то, что степень избыточности в каждом классе ограничивается максимальным числом импульсов, которые можно допустить, но на практике эту информацию не так легко получить. Более того, предложенная схема требует буферизации как на стороне получателя, так и на стороне отправителя. Это приводит к задержкам перед верификацией и вычислением ХФП. Таким образом, предложенное решение может быть неподходящим для большинства медиапотоковых приложений, которые требуют передачи в режиме реального времени.

Выводы

Рассмотренные в работе протоколы аутентификации позволяют проводить аутентентификацию источника данных при наличии помех в каналах связи, приводящих к потере некоторых пакетов. Число потерянных пакетов, не влияющих на аутентификацию сообщения, может быть различно и зависит от выбранного протокола. Полученная хэш-функция позволяет не только убедиться в подлинности каждого пакета, но и обеспечивает неотрекаемость источника сообщения.

Список литературы

1. Конституция України: офіц. текст. – К.: НТУ, 2006. – 80 с.

2. Гринберг А.С. Защита информационных ресурсов государст-венного управления: учеб. пособие для вузов / А.С. Гринберг, Н.Н. Горбачев, А.А. Тепляков. – М.: ЮНИТИ-ДАНА, 2003. – 327 с.

3. Efficient Authentication and Signing of Multicast Streams over Lossy Channels / Perrig et al. // IEEE Symp. Security and Privacy. – 2000. – 246 p.

4. Challal Y. An Adaptive Source Authenti-cation Protocol for MultiCast Streams / Y. Challal, H. Bet-tahar, A. Bouabdallah // IEEE-ISCC'2004. – June 2004. – 236 p.

5. Miner S. Graph-Based Authentication of Digital Streams / Sara Miner, Jessica Staddon // IEEE Symp. Security and Privacy. – 2001. – 164 p.

6. Golle P. Authenticating Streamed Data in the Presence of Random Packet Loss / P. Golle and N. Modadugu // The Network and Distributed System Security Symp. – 2001. – 188 p.

Поступила в редколлегию 5.03.2009

Рецензент: д-р техн. наук, проф. О.А. Серков, Национальный технический университет «ХПИ», Харьков.

ПРОТОКОЛИ БАГАТОАДРЕСНОЇ АВТЕНТИФІКАЦІЇ З ЗАБЕЗПЕЧЕННЯМ НЕВІДМОВЛЕННЯ, ЩО ДОПУСКАЮТЬ ВИТРАТУ ПАКЕТІВ

В.Я. Певнєв, В.В. Торяник, Є.В. Торяник, Г.З. Халімов

Розглянути протоколи багатоадресної автентифікації при наявності завад у каналах зв'язку, які приводять до витрати пакетів. Протоколи, які розглянуто, дозволяють ідентифікувати автора повідомлення та гарантувати його невідмовлення.

Ключові слова: *автентифікація, пакет, протокол, хеш-функція.*

MULTICAST AUTHENTICATION PROTOCOLS WITH NON-REPUDIATION THAT TOLERATES PACKET LOSS

V.Y. Pevnev, V.V. Toryanik, Y.V. Toryanik, G.Z. Khalimov

Multicast authentication protocols with interferences in communication channels that leads to the packet loss were considered. Presented protocols allows to authenticate (identify) the author and to guarantee his non-repudiation.

Keywords: *authentification, package, protocol, хеш-function.*