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*

АНАЛИЗ ПРОТОКОЛОВ МНОГОАДРЕСНОЙ АУТЕНТИФИКАЦИИ БЕЗ ОБЕСПЕЧЕНИЯ НЕОТРЕКАЕМОСТИ

Рассмотрены протоколы многоадресной аутентификации без обеспечения неотрекаемости, произведен их сравнительный анализ, на основании которого сделаны выводы о эффективности этих протоколов.

Ключевые слова: *протокол, код аутентификации сообщения, ключ.*

Введение

Эффективность распространения информации сегодня характеризует уровень развития всех информационных технологий, главной из которых, несомненно, становиться глобальная сеть – Интернет. В современном Интернете имеются следующие существенные проблемы: ограниченное адресное пространство и пропускная способность, неприспособленность к передаче информации, чувствительной к задержкам, сложность широковещательной передачи данных и, наконец, многоаспектные проблемы информационной безопасности. Интернет-технологии традиционно ориентированы на индивидуальное обслуживание, однако весьма ограничены скоростью в мультимедийных источниках. Поэтому актуальной задачей является развитие новых технологий мультикастинга – групповой доставки многоадресных сообщений – широковещания в Интернете. Основная проблема – информационная безопасность. Одним из базовых вопросов информационной безопасности является аутентификация, т.е. процесс проверки подлинности автора. Аутентификация многоадресных источников в реальном времени является активно исследуемой нетривиальной криптографической задачей.

При аутентификации многоадресного источника данных непосредственным решением есть разделение секрета между участниками группы и отправителем. Для аутентификации многоадресного сообщения отправитель вычисляет код аутентификации сообщения (MAC), используя секретный ключ, и передаёт группе участников его вместе с сообщением. При получении переданного сообщения, получатели аутентифицируют источник данных, проверяя полученный MAC с использованием секретного ключа. Недостатком этого решения является то, что все члены группы знают секретный ключ и, следовательно, любой может выдавать себя за отправителя, вычисляя MAC. Поэтому, для обеспечения аутентификации многоадресного источника данных, получатели должны иметь возможность только проверять MAC, не имея возможности его вычисления. Для решения поставленной задачи возможны протоколы с использованием[1]:

- асимметрии секретной информации разделяемой между членами группы пользователей;
- временной асимметрии при разделении секретной информации между членами группы пользователей;
- гибридных схем асимметрии секретной информации и временной асимметрии.

Асимметрия, основанная на секретной информации

Простой протокол. Отправитель разделяет секретный ключ K_i с каждым получателем i. Отправитель знает n секретных ключей $\{K_i, 1 \le i \le n\}$ и каждый получатель i знает только свой секретный ключ K_i. Для аутентификации сообщения m отправитель вычисляет n MAC, используя n секретных ключей, и соединяет их в сообщение: $MAC(K_n, m)|...| MAC(K_1, m)| m$. Каждый получатель i проверяет подлинность принятого сообщения m, используя свой секретный ключ K_i и соответствующий $MAC(K_n, m)$.

Для подделки сообщения от имени правильного отправителя, злоумышленник должен получить секретные ключи других членов для вычисления правильного MAC. Протокол хорошо противостоит сговору, так как даже если n – 1 злоумышленных получателей сотрудничают, то они все равно не смогут навязать сообщение члену группы, не вошедшего в сговор. Недостатком является большой размер аутентификационной информации, который пропорционален числу получателей (n x |MAC|, где n – число получателей и |MAC|-размер MAC) [2].

Для устранения этого недостатка можно множество получателей разделить на p подмножеств. Каждое такое подмножество получателей имеет один секретный ключ с отправителем. Для аутентификации сообщения отправитель вычисляет только p MAC кодов. При получении сообщения и MACов для проверки подлинности полученного сообщения, каждый получатель использует свой секретный ключ, который он разделяет с другими получателями. В этой схемой, размер аутентификатора пропорционален p x |MAC|. Недостатком данной схемы является чувствительность к сговорам.

В [3] представлен протокол, позволяющий найти некоторый компромисс между размером аутентификационной информацией и устойчивостью к сговорам

Аутентификационная схема (k, n) строится на основе полиномиальной схемы. Источник генерирует полином $A_M(x)$ степени k для сообщение M. Каждому получателю посылается разделённый полином. Чтобы подделать аутентификатор сообщения, необходимо иметь не менее k частей полинома для его восстановления. Так как самое большое объединение мошеннических получателей может иметь только k-1 членов, тем самым обеспечивается безопасность системы. Основные шаги предложенного протокола:

1) отправитель выбирает большое простое число p, где p больше или равно числу возможных сообщений. Все вычисления выполняются в конечном поле Z_p;

2) для каждого сообщения M отправитель формирует два полинома $P_0(x)$ и P'(x) степени k;

3) отправитель лично передаёт значения $P_0(i)$ и P'(i) каждому получателю (i);

4) отправитель генерирует аутентификатор (полиномиальный) сообщения $M:A_M(x) = P_0(x) + MP'(x)$ и посредством групповой передачи передаёт его получателям;

5) получатели проверяют аутентификатор, вычисляя $A_M(i) = P_0(i) + MP'(i)$.

Достоинства и недостатки. В работе [3] показано, что этот протокол есть k из n безусловно секретной схемой аутентификации. Протокол допускает потерю пакета, так как каждый пакет содержит свою аутентификационную информацию и, следовательно, может быть проверен независимо от других пакетов. Каждое сообщение содержит аутентификатор размера $(k+1)\cdot\log_2 p$ бит. На приемной стороне получатели должны хранить $2\cdot\log_2 p$ бит аутентификационных данных, соответственно, на передающей стороне $2(k+1)\cdot\log_2 p$ бит. Доказано, что k получателей не могут совершит атаку замены или выдачи себя за другое лицо с вероятностью превышающую 1/p.

S. Obana и K. Kurosawa [4] представили нижнюю оценку вероятности подделки сообщений в зависимости от числа ключей *k* в *n* пользовательской аутентификационной схеме и показали, что схема, предложенная Desmedt и др. удовлетворяет этим границам с равенством. Это позволяет сделать вывод, что предложенная схема аутентификации является оптимальной. Однако эти схемы не практичны из большого объема аутентификационной информации.

Safavi-Naini и Wang [5, 6] обобщили полиномиальную схему таким образом, что вместо одиночного сообщения каждый полином может использоваться для аутентификации множества сообщений. В [7] предложена безусловно безопасную схему широковещательной аутентификации, основанную на системе множеств без покрытия. Все множество ключей, используемых отправителем для аутентификации сообщений, распределяется среди получателей таким образом, что j мошеннических получателей ($j < k$) не смогли бы сотрудничать, используя каждый свое подмножество ключей для вычисления ключевого покрытия для члена группы. В работе [7] представлены комбинированные границы вероятности подделки и предлагают конструкции, которые удовлетворяют этим границам.

В работах [8, 9] представлены протоколы, обеспечивающие решения условно безопасной многоадресной аутентификации. Условная безопасность предполагает, что атакующий не имеет достаточно вычислительных ресурсов, чтобы за приемлемое время вычислить секретные ключи, использующиеся для аутентификации сообщений.

Canetti и др. [8] рассмотрели протокол, суть которого состоит в том, что отправитель добавляет к каждому многоадресному сообщению M, *l* MAC кодов, используя *l* различных ключей. Каждый получатель владеет подмножеством ключей из числа *l* ключей отправителя и проверяет подлинность полученных сообщений, используя своё подмножество ключей. Для противника, чтобы подделать сообщение правильного отправителя, необходимо завладеть *l* ключами из объединения w получателей. Краеугольным камнем этого решения есть то, что соответствующий выбор подмножества ключей получателей гарантируется, что с большой вероятностью не существует коалиции больше *w* плохих членов (где w-параметр), знающих все ключи, имеющиеся у пользователя и, таким образом, обеспечивается аутентичность.

Основные шаги протокола (здесь S – источник передачи, а u — получатель в многоадресной группе):

- S хранит набор R из *l* ключей, $R = \{K_1,\ldots, K_l\}$;
- каждый получатель знает свое подмножество из этих ключей;
- когда S посылает сообщение, он в первый раз аутентифицирует его с каждым из *l* ключей, которые он хранит, используя MAC. Затем он посылает сообщение M вместе с $MAC(K_1, M) \mid MAC(K_2, M)|\ldots| MAC(K_l, M)$;
- каждый получатель проверяет все MAC, которые были созданы, используя ключи из своего подмножества R_u;
- если хотя бы один из этих ключей не найдет свою пару, то сообщение отвергается.

Безопасность протокола определяется вероятностью того, что подмножества ключей мошеннической коалиции полностью покрывают подмножество ключей R_u данного пользователя u. Для верхней оценки этой вероятности равной q, авторы предлагают, чтобы отправитель использовал $l = 4e^{w\ln l/q}$ ключей, где w – размер самого большого объединения и что каждый ключ меняется в подмножестве пользователя с вероятностью $1/(w + 1)$. В соответствии с этой конструкцией, авторы доказывают, что если вероятность вычисления выхода MAC без знания ключа равняется не более q', тогда вероятность того, что объединение w мошеннических пользователей могут аутентифицировать сообщение M, предназначающееся получателю u, равняется не более q+ q'.

Предложенное решение позволяет относительно эффективно генерировать и верифицировать аутентификационную информацию, так как оно основывается только на вычислениях MAC, которые эффективны для генерации и проверки. Авторы предлагают использовать MAC с единственным битом в качестве выхода. Следовательно, аутентификационная информация уменьшается до *l* битов. В [9] показано, что протокол Canetti и др. имеет оптимальную длину аутентификатора. Каждый пакет содержит свою аутентификационную информацию и, следовательно, каждый пакет может проверяться индивидуально. Таким образом, данный метод допускает потерю пакетов. Главным недостатком данного метода есть то, что он остаётся уязвимым к сговору плохих членов.

Временная асимметрия

В протоколах этой категории ограничивается время жизни ключей, использующихся для аутентификации многоадресных пакетов. Отправитель генерирует ключи периодически для аутентификации многоадресных пакетов за промежуток времени. Если противник использует ключ для вычисления аутентификационной информации сообщения от лица отправителя, то получатели отвергнут сообщение, потому что истёк срок действия ключа.

Основные решения протоколов рассматривают аутентификацию самих ключей и их генерацию.

Механизм генерации ключей на основе односторонних цепочек. Главная идея односторонних цепочек состоит в сертификации (например, на основе цифровой подписи) только одного секрета. Этот сертифицированный секрет является результатом односторонних рекурсивных вычислений, которые формируют всю цепочку. Для генерации цепочки длины k, отправитель выбирает последний элемент цепочки K_k. Затем он генерирует цепочку, многократно применяя одностороннюю функцию H. Последнее значение K_0 ,будет секретом, который должен быть послан безопасно (сертифицировано) получателям. Затем секреты воспроизводятся в обратном порядке. Для проверки, является ли полученный секрет K_i истинным (т.е., что он действительно исходит от отправителя) получатель секрета проверяет, что $H^i(K_i) = K_0$.

Первый протокол данной категории предложен Bergadano и др. [10]. Суть протокола состоит в аутентификации каждого пакета данных с помощью MAC, используя ключ, сгенерированный на основе односторонних цепочек. Рекурсивная зависимость между ключами делает возможным восстановление потерянных ключей и проверки правильности полученных ключей. Пакеты с MAC кодами и использованные для этих целей ключи, посредством многоадресного вещания передаются получателям. Чтобы мошеннические получатели не использовали полученный ключ для подделки пакетов данных от имени легитимного отправителя, отправитель гарантирует, что ключи будут известны получателям, только когда все получатели получат пакеты, аутентифицированные с помощью их соответствующих ключей. Поэтому, получатели синхронизируются с часами отправителя, и им поручается отвергать любые пакеты данных, чьи MAC пришли позже.

Протокол Bergadano минимизирует размер аутентификационной информации до одного MAC на пакет данных. Допускается потеря пакета, также как и потеря ключа. Синхронизация получателей с часами отправителя остаётся главным недостатком метода. Кроме этого, длина односторонней ключевой цепи ограничена и, следовательно, используя аутентификацию с неограниченным потоком, отправителю необходимо будет совершать периодическое обновление односторонней ключевой цепи и её оповещение.

Широковещательный аутентификационный протокол TESLA был предложен в [11,12]. Суть этого протокола состоит в том, что отправитель использует разные ключи в каждый промежуток времени для аутентификации многоадресных сообщений в этот промежуток времени. TESLA использует одноразовые ключевые цепи для генерации MAC ключей. Секретный MAC ключ, сохраняется отправителем в секрете, чтобы избежать получения ключа атакующим, до того как его получат правильные получатели. По истечении периода времени, соответствующего использованию этого ключа, отправитель его открывает. Получатели используют этот ключ для проверки подлинности ранее полученных сообщений. Если атакующий использует этот ключ для подделки сообщений от имени отправителя, получатели отвергнут это сообщение, потому что они синхронизировали свои часы с часами отправителя, и они знают, что отправитель передаст другой ключ, соответствующий следующему интервалу времени.

В протоколе TESLA размер аутентификационной информации уменьшается до размера одного MAC. В противоположность протоколу Bergadano, TESLA открывает единственный MAC ключ за период времени. Пакеты могут быть индивидуально аутентифицированы и, следовательно, протокол допускает потерю пакетов. Кроме того, если ключ потерян, то сцепление, используемое в конструкции, делает возможным восстановление потерянного ключа из последующих ключей. Главным недостатком TESLA есть его требование синхронизации между источником и получателями, которое создает новую потенциальную дыру в безопасности для противников. Применение протокола TESLA требует, чтобы полученные пакеты были буферизированы до тех пор, пока соответствующие ключи не будут открыты и, следовательно, они не могут быть использованы ресурсоограниченными устройствами или приложениями, которые требуют передачи в реальном времени.

Расширения и улучшения протокола TESLA были предложены в ряде робот. Так в [11] рассмотрена модификация, которая позволяет аутентифицировать большинство пакетов, без буферизации за счет некоторого увеличения аутентификационной информации. В [13] предложена облегченная версия μTESLA для специальных сенсорных сетей, которые, как известно, являются очень ограниченными в ресурсах.

Гибридная асимметрия

Главная идея, предложенная в [13] заключается в том, что отправитель использует множество ключей для аутентификации сообщений. Когда отправитель аутентифицирует сообщение, он открывает только подмножество ключей, которое позволяет проверять аутентификационную информацию пакета без генерации секретной ключевой информации. Подлинность пакетов проверяется, как только они будут получены и это соответствует подходу асимметрии, основанной на асимметрии секретной информации. Но, если один и тот же набор ключей используется для аутентификации определённого числа пакетов, каждый получатель, в конце концов, получит весь набор ключей отправителя после открытия некоторого подмножества, что предоставляет возможность подделывать сообщения от имени правильного отправителя. Чтобы избежать этого, отправитель периодически меняет набор ключей, использующихся для аутентификации сообщений. Генерация ключей использует механизм односторонней ключевой цепи так, чтобы получатели могли верифицировать их аутентичность и могли восстанавливать их всякий раз, когда некоторые из них потеряны. Это обеспечивается с помощью метода временной асимметрии. Таким образом, предложенная схема является гибридом из двух подходов, описанных ранее и устраняющая их недостатки.

Perrig в [13] предложил протокол гибридной асимметрии, используя новую одноразовую сигнатурную схему, называемую BiBa (Bins и Balls).

Одноразовая подпись BiBa. Методология подписи BiBa основывается на принципиально новом подходе: использовании эффекта коллизий. Схема алгоритма является следующей:

- для сообщения m подписывающий вычисляет хэш $h = H(m|c)$, где c – значение счетчика, которое увеличивается до тех пор, пока не будет найдена подпись для этого сообщения;
- отправитель применяет хэш-функцию G_h ко всему набору секретных ключей $S_1,S_2,\ldots, S_t$ (где G_h – экземпляр хэш семейства G, выбранный с индексом h);
- находятся ключи $S_i \neq S_j$ при которых возникает двухсторонняя коллизия $G_h(S_i) = G_h(S_j)$;
- если двухсторонняя коллизия не случилась, то отправитель увеличивает счётчик *c* и процесс поиска продолжается;
- подпись формируется двусторонними коллизионными ключами $< S_i, S_j >$, сцепленными со счётчиком c;
- проверяющий получает сообщение m и BiBa подпись $< S_i, S_j > | c$. Для проверки BiBa подписи, вычисляется $h = H(m | c)$ с проверкой, что при $S_i \neq S_j$ справедливо $G_h(S_i) = G_h(S_j)$.

В данной схеме противнику открывается небольшое число ключей, которые участвуют в подписании и следовательно есть малая вероятность того, что на этом множестве ключей можно подделать подпись для нового сообщения. Perrig показал [13], что если подмножество ключей, используемых для нахождения коллизий уменьшается, то вероятность того, что возникнет коллизия, уменьшается экспоненциально. Для повышения безопасности, в предложенной схеме рассматривают k-стороннюю коллизию.

В широковещательном протоколе аутентификации BiBa открывают k из t ключей секретного набора как подпись для каждого сообщения. Получатели проверяют подпись, как только она получена вместе с сообщением. Чтобы устранить ситуацию, когда после определённого числа передач получатели получат все секретные ключи, отправитель вводит разные наборы ключей по истечении некоторого промежутка времени. Для предотвращения возможности мошенническому получателю восстанавливать весь набор ключей, а, следовательно, и возможность подделки одноразовых подписей, отправитель не должен открывать более некоторого порога ключей за некоторый промежуток времени.

В протоколе BiBa допускается потеря пакетов, так как каждый пакет сопровождается вместе со своей BiBa подписью независимо от других пакетов и, даже если некоторые ключи, которые составляют подпись, будут потеряны, они могут быть восстановлены из последующих полученных ключей, используя односторонние цепи. BiBa не уязвим к сговорам злоумышленных получателей, так как отправитель задействует новый набор ключей после каждого промежутка времени. Схема одноразовой подписи BiBa имеет размер одноразовой подписи меньший, чем у других одноразовых подписей. Каждая генерация подписи требует 2^{t+1} хэш-вычислений, где t – порядка 1024 бит. Время, необходимое для генерации подписей велико. Также требуется посылка получателям большого числа открытых ключей, каждый из которых имеет размер 10 Кбайт, что является узким местом протокола. Широковещательный протокол аутентификации BiBa требует, чтобы отправитель и получатели были синхронизированы по времени.

L. Reyzin и N. Reyzin предложили схему одноразовой подписи, базирующуюся на односторонней хэш функции, которая быстрее BiBa при проверке [14]. Подписание выполняется быстрее, чем её проверка, размеры ключа и подписи немного улучшены. Таким образом, предложенная схема одноразовой подписи сохраняет достоинства одноразовой схемы подписи BiBa и устраняет её основные недостатки.

Сравнительные оценки рассмотренных протоколов многоадресной аутентификации представлены в табл. 1.

Таблица 1

Анализ протоколов аутентификации по стойкости безопасности и качеству обслуживания

Протокол	Уровень безопасности	Уязвимость к стоворам	Задержки у источника	Задержки у получателя	Допустимость потери пакетов	Размер аутентификационной информации	Требование синхронизации
Desmedt и др.	Безусловная	+	Нет	Нет	Да	$(k+3)\times\lceil \log_2 p \rceil$ бит, где p – большое простое число больше или равное числу сообщений	Нет
Canetti и др	Условная	+	Нет	Нет	Да	l бит, где l зависит от размера самой большой коалиции злоумышленных пользователей	Нет
Bergadano и др	Условная	–	Нет	Да	Да	$\lvert MAC \rvert + \lvert k_m \rvert$	Да
TESLA	Условная	–	Нет	Да	Да	$\lvert MAC \rvert \left[+\lvert k_m \rvert\right]$, где k_m открывается только один раз за промежуток времени	Да
BiBa	Условная	–	Нет	Нет	Да	$k\times\lvert ball \rvert+\lvert counter \rvert\left[+\lvert k_m \rvert\right]$, где k порядка 15, $\lvert ball \rvert$ порядка 64 бит	Да

Основные результаты анализа

Устойчивость к потере пакетов. Большинство из протоколов, которые обеспечивают аутентификацию многоадресного источника данных, допускают потерю пакетов, потому что каждый пакет несёт в себе свою собственную аутентификационную информацию, независимо от других пакетов. Предложенные протоколы основываются на быстрых криптографических механизмах для обеспечения аутентификации источника данных. Протоколы Canetti и др., Bergadano и др., TESLA используют MAC коды, а BiBa использует одноразовые подписи. Отправитель вычисляет аутентификационную информацию для каждого пакета, которую можно индивидуально проверять. Безусловно, безопасные схемы широковещательной аутентификации, такие, как схемы, базирующиеся на полиномах, предположенные Desmedt и др. также допускает потерю пакетов. Однако вычисления, требуемые для генерации аутентификационной информации для каждого пакета, являются очень сложными.

Передача в реальном времени. TESLA и решения, предложенные Bergadano и др., страдают от того, что получатели должны буферизировать полученные пакеты, до тех пор, пока соответствующий верификационный ключ не открыт отправителем. Иное решений – это протокол, предложенный Canetti и др., аутентификация и верификация ограничивается только моментом MAC вычислений (без задержек). Однако, это решение может использоваться только в средах, где коалиция определённого числа мошеннических пользователей невозможна. В протоколе BiBa аутентификационная информация генерируется и проверяется немедленно (без ожидания другой информации) и она нечувствительна к коалициям. Однако, процесс генерации аутентификационной информации относительно медленный (в сравнении с решением Canetti и др.).

Пропускная способность. Оптимальным решением является TESLA. Расходы на пропускную способность, вызванные TESLA уменьшаются до одного MAC (порядка 128 бит, используя MD5) в дополнение к открытию одного ключа за промежуток времени. Решение, предложенное Bergadano и др. имеет те же самые расходы на пропускную способность (один MAC на пакет), но оно также имеет открытие одного ключа на пакет. Эти решения требуют, чтобы получатели были синхронизированы по времени с отправителем. Другим решением с относительно низкой пропускной способностью и без последнего недостатка есть протокол, предложенный Canetti и др, который основывается на асимметрии множественных MAC кодов. Расход на пропускную способность, порождаемый этим протоколом равняется l MACов на пакет, где l зависит от размера самой большой коалиции мошеннических получателей, которая существует в данной сессии.

В их примере Canetti и др. показали, что l может быть выбрано порядка 190 MAC кодов из 10 бит в основной схеме, 380 MAC кодов из 10 бит в улучшенной по безопасности схеме, или порядка 760 MAC кодов из 1 бита в схеме с низкими коммуникационными расходами. В протоколе BiBa подпись пакета уменьшается до k ключей по 64 бит, где k порядка 10-16. Однако, проблемой BiBa есть то, что требуется большая ширина канала для распространения открытого ключа (который имеет размер порядка 10 Кбайт) всем пользователям. Обычно, когда сессия динамическая, новые члены могут присоединяться к сессии свободно и каждому новому члену требуется получить открытые ключи всех запущенных экземпляров BiBa. В этом случае распространение открытых ключей может привести к узкому месту в протоколе [15].

Ресурсоемкость. Протокол BiBa не является подходящим решением для сред с ограниченными ресурсами. Сложные вычисления, безусловно, безопасной аутентификации на основе полиномиальной схемы, предложенной Desmedt и др., также не подходит для

этого вида сети. Решение, предложенное Canetti, требует низких расходов на хранение аутентификационных данных: отправитель сохраняет *l* MACов и каждый получатель сохраняет (*l* / w + 1) MAC, где w – самая большая коалиция мошеннических пользователей, которая может существовать в сессии. Лучшими протоколами по требования вычислительной мощности, являются TESLA и решение, предложенное Bergadano и др. Действительно, оба этих решения уменьшают генерацию и верификацию аутентификационной информации до вычисления одного MAC. Однако эти два протокола страдают от требования буферизировать пакеты, полученные в определённый промежуток времени, вдобавок к ключу подписи у получателей. Кроме того, отправитель может управлять длинными односторонними цепочками MAC ключей. В случае TESLA, промежуток времени и, следовательно, требования буферизации на стороне получателя более значительные, чем в Bergadano и др. Однако Bergadano и др. требует, чтобы отправитель управлял длинными цепочками MAC-ключей, так как каждый ключ используется для аутентификации только единственного пакета.

Мобильность. На практике протоколы, базирующиеся на временной асимметрии, не подходят для высоко динамичных сетей, когда узлы свободно присоединяются и покидают сессию, а топология сети может измениться через время. В сущности, протоколы TESLA, BiBa и Bergadano и др. предполагает, что получатели синхронизированы с отправителем, так что получателям гарантируется, что все из них получат аутентифицированные пакеты, перед тем, как будет раскрыт соответствующий MAC ключ. Для разрешения проблемы мобильности узлов необходимо пересчитывать промежуток времени открытия ключей отправителем после каждой задержки, что является слабым местом протоколов [16] .

Выводыя

В представленной работе произведен анализ существующих протоколов многоадресной аутентификации. При проведении анализа рассматривались рассмотренные в статье протоколы. Сравнительный анализ этих протоколов проводился по следующим параметрам: устойчивости к пропаданию пакета, пропускной способности, времени передачи, ресурсоемкости, мобильности.

Списокяитературыя

1. Шульте В. Протокольно-независимая многоадресная рассылка / В. Шульте // Журнал сетевых решений LAN. – [Электронный ресурс]. – Режим доступа к статье: /www.osp.ru/lan/2005/12/377592.

2. Халимов Г.З. Методы и средства аутентификации многоадресного источника данных / Г.З. Халимов, А.А. Дунь // Прикладная радиоэлектроника. – 2007. – № 3. – С. 377-386

3. Desmedt Y. Multi-receiver/Multisender Network Security: Efficient Authenticated Multicast/Feedback / Y. Desmedt, Y. Frankel, M. Yung // IEEE INFOCOM'92. – 1992. – P. 2045-54.

4. Obana S. Bounds and Combinatorial Structure of (k, n) Multi-receiver A-codes / S. Obana, K. Kurosawa // Designs, Codes andCryptography. – 2001. – Vol. 22, No. 1. – P. 47-63.

5. Safavi-Naini R. New Results on Multi-receiver Authentication Codes," / R. Safavi-Naini, H. Wang // Advances in Cryptology: EU ROCRYPT'98. – 1998. – LNCS vol., No. 1403. – P. 527-41.

6. Safavi-Naini R. Multireceiver Authentication Codes: Models, Bounds, Constructions, and Extensions / R. Safavi-Naini, H. Wang // Information and Computation. – 1999. – Vol. 151. – P. 148-72.

7. Fujii H. Combinatorial Bounds and Design of Broadcast Authentication / H. Fujii, W. Kachen, K. Kurosawa // IEICE Trans. – 1996. – E79- Avol., No. 4. – P. 502-506.

8. Multicast Security: A Taxonomy and Efficient Constructions / R. Canetti et al. // INFOCOM. – 1999. – P. 340.

9. Boneh D. Lower Bounds for Multicast Message Authentication / D. Boneh, G. Durfee, M. Franklin // Eurocrypt '01. – 2001. – LNCSvol., No. 2045. – P. 437-52.

10. Bergadano F. Individual Single-Source Authentication on the Mbone / F. Bergadano, D. Cavagnino, B. Crispo // IEEE Int'l. Conf. Multimedia and Expo. – 2000. – P. 450.

11. Efficient Authentication and Signing of Multicast Streams over Lossy Channels / A. Perrig et al. // IEEE Symp. Security and Privacy. – 2000. – P. 233.-35.

12. The TESLA Broadcast Authentication Protocol / A. Perrig et al. // RSA CryptoBytes. – Summer 2002. – Vol. 5. – P. 441-54.

13. SPINS: Security Protocols for Sensor Networks / A. Perrig et al. // Wireless Networks. – 2002. – Vol. 8. – P. 521-34.

14. Perrig A. The BiBa One-time Signature and Broadcast Authentication Protocol / A. Perrig // 8th ACM Conf. Comp. and Commun. Security. – Nov. 2001. – P. 641-52.

15. Алгоритмы шифрования – финалисты конкурса AES. – [Электронный ресурс]. – Режим доступа к статье: www.ixbt.com/soft/alg-encryption-aes.shtml.

16. Библиотека криптографических преобразований. – [Электронный ресурс]. – Режим доступа к статье: http://vmssoft.com/ contact.php?link= sus&leng=1.

Поступила в редколлегию 16.10.2008

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

АНАЛІЗ ПРОТОКОЛІВ БАГАТОАДРЕСНОЇ АВТЕНТИФІКАЦІЇ БЕЗ ЗАБЕЗПЕЧЕННЯ НЕВІДМОВЛЕННЯ

В.Я.Пєвнєв, В.В.Торяник, Е.В.Торяник, Г.З.Халимов

Розглянуто протоколи багатоадресної автентифікації без забезпечення невідмовлення, проведено їх порівняльний аналіз, на підставі котрого зроблені висновки щодо ефективності цих протоколів.

Ключові слова: *протокол, код аутентифікації повідомлення, ключ.*

THE ANALYSIS OF PROTOCOLS FOR MULTI-ADDRESS AUTHENTICATION WITHOUT NON-REFUSE PROVIDING

V.Ya. Pevnev, V.V. Toryanik, E.V. Toryanik, G.Z. Khalimov

The protocols for multi-address authentication without non-refuse providing are studied, the analysis comparizon of protocols was done. The conclusion about efficiency of protocols was made.

Keywords: *protocol, code of authentification of report, key.*