УДК 510.645:004.032.26

[1]**Печурин Н.К.,** д.т.н. проф.,
[2]**Кондратова Л.П.,** к.т.н.,
[1]**Печурин С.Н.,** к.т.н.

МОДЕЛИРОВАНИЕ БЕЗОПАСНОГО ВНУТРИУРОВНЕВОГО ВЗАИМОДЕЙСТВИЯ В БЕСПРОВОДНОЙ КОМПЬЮТЕРНОЙ СЕТИ СРЕДСТВАМИ ТЕОРИИ ФОРМАЛЬНЫХ ГРАММАТИК И ЯЗЫКОВ

[1]Национальный авиационный университет
[2]Национальный технический университет Украины «КПИ»

pechnk@mail.ru

Способ описания трансляции протокольных модулей данных в процессе перехода между подуровнями PMD и PLCP физического уровня эталонной модели взаимодействия открытых систем, основанный на моделях регулярных грамматик и языков, обеспечивает адекватное представление этого взаимодействия. Предлагается, с целью моделирования безопасного взаимодействия указанных подуровней, рассматривая их как взаимодействующие объекты в защищённой системе передачи информации, применить вышеуказанные модели с ослабленными ограничениями, где на продукционные правила не накладывается ограничение регулярности, и они выступают в качестве составных частей прямонаправленной функции асимметричной системы шифрования

Ключевые слова: безопасное внутриуровневое взаимодействие, асимметричная криптосистема, прямое и обратное преобразование протокольных модулей, модели регулярной грамматики метаязыка, модель однонаправленного отображения

Введение

Наличие неконтролируемых областей между конечными пользователями компьютерной беспроводной сети приводит к большему числу угроз по сравнению с проводными сетями [1]. Этот факт обусловил необходимость усиления механизмов защиты и безопасности передаваемой информации. Конфиденциальность и целостность информации в беспроводных сетях стандартов IEEE 802.11, IEEE 802.16-2001, IEEE 802.16e-2005 и подобных обеспечивается средствами физического уровня, идентификации набора служб, управления доступом к среде передачи, механизмами *WEP* и *WPA* аутентификации и шифрования. Средства защиты информации, реализуемые механизмами *WEP*, *WPA*, *WPA2*, направлены на предотвращение несанкционированных точек доступа. В работах [2, 3] описан метод защиты беспроводных сетей, основанный на новом принципе работы сетевого протокола: предполагается введение, для реализации функций защиты, дополнительных функций и даже целого (крипто-) уровня, располагаемого между сетевым и транспортным уровнями в иерархической эталонной модели взаимодействия открытых систем (ЭМ ВОС). Эффективность криптографической защиты могут обеспечивать асимметричные криптосистемы (криптосистемы с открытым ключом) [4]. Шифрование сообщений в таких системах выполняется на основе однонаправленных функций

$$E_{K_1} : M \to C, \quad D_{K_2} : C \to M$$

(M, C - сообщение и криптограмма соответственно) с ключами K_1 и K_2. Особенностью асимметричных криптосистем является сложность обратного преобразования $D_{K_2} : C \to M$, обусловленная секретностью ключа K_2. Однонаправленная функция чаще всего представляется модульной экспонентой с фиксированным основанием и модулем в виде: $C=M^{K1}$ для прямого преобразования, $M=C^{K2}$ для обратного преобразования. Шифрование $E_{K_1} : M \to C$

и дешифрование $D_{K_2} : C \to M$ в асимметричной системе выполняются по схеме рис.1 [4, 5].

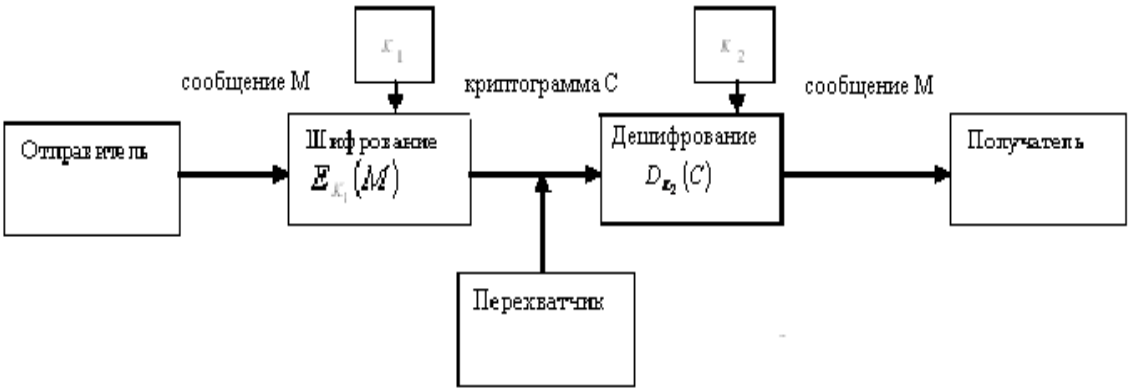

Рис.1. Схема шифрования-дешифрования в асимметричной криптосистеме с открытым ключом

В работе [6] рассмотрен подход к переклассификации функций ЭМ ВОС для адекватного межуровневого преобразования данных на основе моделей контекстно-свободных языков. Данный подход предлагается применить для адекватного представления безопасного взаимодействия протокольных модулей данных (*PDU)* подуровней *PLCP* и *PMD* физического уровня ЭМ ВОС.

Постановка задачи

Трансляция *PDU* в процессе перехода от подуровня *PLCP* к подуровню *PMD*, на передающей стороне системы компьютерного взаимодействия, осуществляется в соответствии с указанными протоколами; эти же протоколы регламентируют обратный переход (от подуровня *PMD* к подуровню *PLCP)* на приёмной стороне. Для описания (моделирования) этих преобразований *PDU* используем инструментарий теории формальных языков и грамматик. Тогда процесс трансляции описывается процедурой (алгоритмом) генерирования предложений регулярного языка с помощью линейных продукционных (в контексте ЭМ ВОС – протокольных) грамматических правил. Конкретное сгенерированное предложение языка суть последовательность битов. Обратное преобразование, на приёмной стороне, описывается процедурой грамматического разбора поступившего предложения. Однозначность этих (функциональных по сути) преобразований обеспечена (в модели) выбором фиксированного типа грамматики (регулярной, контекстно-свободной и пр.), установлением фиксированной последовательности применения правил продукции как при генерировании предложений из терминальных символов (передающая сторона), так и восстановления предложений из символов алфавита *PLCP* в процессе грамматического разбора (приёмная сторона).

Однозначность преобразований в соответствии с протоколами *PLCP* и *PMD* , моделируемая так, как это сказано выше, не обеспечивает безопасного взаимодействия подуровней, точнее, - уровень безопасности соответствует *QoS* ЭМ ВОС.

Сделаем предположение, что из каких-то соображений в механизм преобразований *PDU* при переходе от подуровня к подуровню включается система защиты информации (данных), то есть теперь на передающей стороне подуровень *PMD* рассматривается как получатель информации, а подуровень *PLCP* – как источник информации в защищённой системе передачи информации (на приёмной стороне подуровни меняются ролями).

Задача заключается в том, чтобы выявить, какие изменения следует сделать в представленной выше модели (основан-

ной на использовании инструментария теории регулярных языков и грамматик), чтобы описать защищённую систему внутриуровневого взаимодействия.

Математические модели преобразования протокольных модулей данных

Взаимодействие протокольных модулей данных подуровня *PLCP* физического уровня (*PPDU*) в беспроводной компьютерной сети описывается математической моделью на основе совокупности леволинейных и праволинейных правил регулярной грамматики для метаязыка ЭМ ВОС [7].

Грамматика представляется четверкой $G=<V_T,V_H,\sigma,P>$ (V_T - алфавит терминальных символов, включающий обозначения для задаваемых параметров: *LH* в заголовках фрейма, *FCS* для контрольной суммы, *A,B,C* для тела фрейма; V_H={*PPDU*, *HEADER, DATA*, *TRAILER*, *SS*} - алфавит нетерминальных символов, используемых в левой части правил множества *P*), $\sigma=PPDU\ \epsilon\ V_H$ - начальный нетерминальный символ). Множество *P* включает следующие правила преобразования *PPDU* для метаязыка ЭМ ВОС:

PPDU→*HEADER PPDU*| *HEADER DATA TRAILER*; (1)

HEADER →*SS LH FCS*|*SS LH*; (2)

SS→0SS1|0SS|1SS|ε; (3)

DATA →*A*|*B*|*C*...; (4)

TRAILER →*FCS*; (5)

где ε – обозначение пустой цепочки.

Процесс обратного преобразования протокольных модулей *PPDU* описывается математической моделью, представляемой на основе совокупности правил множества *P* конечным автоматом в виде $<V_T,A,V_H,\delta,P>$, где $A=\{a_1, a_2, \ldots, a_n\}$ – множество состояний, δ – функция перехода как отображение вида

$$\delta : A\times V_T \to A \left| \delta(a_{k-1}, V_T) = a_k,\ \ k=\overline{2,n}. \right. \qquad (6)$$

Процедура преобразования PPDU

Процедура преобразования протокольных модулей данных подуровня PLCP суть формирование (операция конкатенации и замена нетерминальных символов терминальными) последовательности символов из V_T; она реализуется многократным применением правил (1)-(5), начиная с начального нетерминального символа $\sigma=PPDU$.

Таким образом, в результате преобразования протокольных модулей данных для физического уровня по продукционным правилам (1)-(5) (регулярной) грамматики порождаются предложения метаязыка ЭМ ВОС (рис.2).

На рисунке процесс применения правил из *P* представлен деревом, где вершины характеризуют составляющие предложений метаязыка.

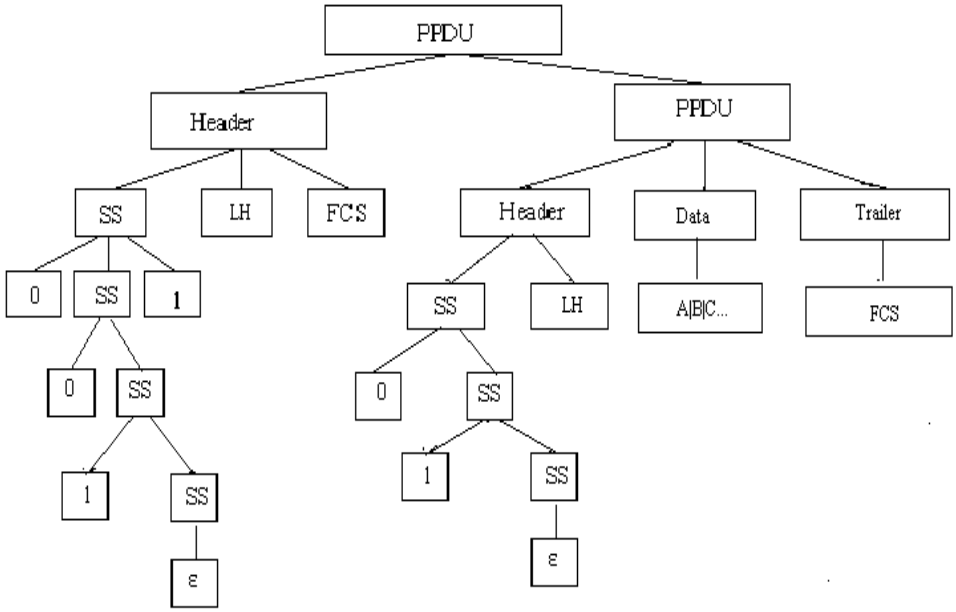

Рис.2. Дерево грамматического разбора предложения физического уровня

Результатом обратного перехода, от нижних к верхним уровням и подуровням ЭМ ВОС на приёмной стороне, является грамматический разбор полученных предложений метаязыка. Процедура грамматического разбора предложения физического уровня выполняется на основе тех же пяти правил (регулярной) грамматики G с использованием функции отображения (6), с определением в результате начального нетерминального символа σ=*PPDU* (рис. 3).

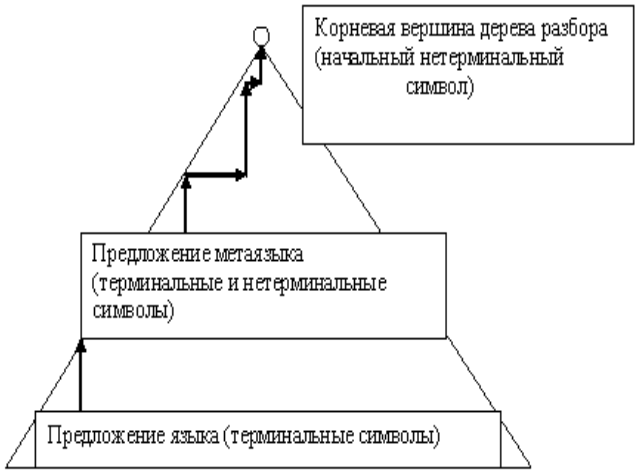

Рис. 3. Одна стратегия поиска корневой вершины дерева разбора (формирования предложения метаязыка)

В качестве примера рассмотрим процедуру трансляции модуля *PDU*, используемого в технологии *DSSS* [6]. Преобразование фрейма в последовательность битов выполняется с использованием схемы *CCK* дополнительных кодов и

механизма шифрования *WEP* на *MAC*-уровне, учитывая скорости передачи, предоставляемые стандартом 802.11b. Использование правил (2), (3) для заголовков физического и канального уровней обеспечивает последовательности, соответствующие скоростям передачи 5,5 Мбит/с и 11 Мбит/с, регламентированным в высокоскоростной технологии *DSSS*. В результате подстановок по правилам (2), (3) цепочки терминалов для заголовка физического уровня длинного и короткого форматов с указанием скорости передачи, равной 5,5 Мбит/с, представляются соответственно в виде:

$$\underbrace{11\ldots1}_{128}1111001110\quad 1000000011\quad 0111000000\quad LHFCS\ ,\ \underbrace{11\ldots1}_{56}0000\ 0101\ 1100\ 1111001101\quad 11000000LH\quad FCS \qquad (7)$$

Ряд подстановок, соответствующих скорости передачи, равной 11 Мбит/с, приводит цепочки терминалов для заголовка длинного и короткого форматов к виду:

$$\underbrace{11\ldots1}_{128}1111001110\ 1000000110\ 1110000000\ LHFCS\ ,\ \underbrace{11\ldots1}_{56}0000\ \ 0101\ 1100\ 1111011011\quad 10000000LH\quad FCS\ . \qquad (8)$$

Цепочки терминалов (7), (8) содержат последовательности битов, в которых равные нулю 154-й и 82-й биты определяют кодирование по схеме *CCK*. Аналогично сформированные цепочки терминалов для заголовка *MAC*-фрейма содержат в последовательности битов равный 1 параметр, определяющий механизм *WEP* шифрования.

Таким образом, процесс преобразования информации в направлении от верхних уровней (подуровней) к нижним представляется моделью порождения предложений языка по продукционным правилам (1-5). Процесс обратного перехода, от нижних уровней (подуровней) к верхним на приёмной стороне, представляется моделью грамматического разбора *PPDU* (полученных предложений). Разбор предложения, полученного на нижнем уровне, т.е. поиск корня дерева грамматического разбора, по сути, является процессом обратного отображения (функции) информации надприкладного уровня в предложения физического уровня. Из-за наличия большого числа степеней свободы в поиске корня дерева грамматического разбора (рис. 3), процедура поиска приобретает все черты поиска аргумента однонаправленной функции Это обстоятельство, с точки зрения защиты, позволяет рассматривать систему преобразования информации: высший подуровень *PLCP* – низший подуровень *PMD* как асимметричную криптосистему [5].

Выводы

Использование инструментария регулярных грамматик для преобразования протокольных модулей данных беспроводной компьютерной сети дает возможность адекватного представления межуровневого преобразования в процессе перехода между *PLCP* и *PMD* физического уровня ЭМ ВОС. Описанный способ преобразования протокольных модулей данных, включающий формирование предложений на физическом уровне и грамматический анализ полученных предложений на основе регулярной грамматики с леволинейными и праволинейными правилами, обеспечивает представление безопасного межуровневого взаимодействия в процессе переходов на физическом уровне ЭМ ВОС для беспроводных компьютерных сетей. Предложенная модель однонаправленного отображения может дать возможность построения алгоритмов

асимметричных криптографических систем.

Список литературы

1. Рошан П., Лиэри Дж. Основы построения беспроводных локальных сетей стандарта 802.11. – М.: Издательский дом «Вильямс», 2004. – 304 с.

2. Лисецкий Ю.М., Бобров С.И. WiMAX сети. Реализации и перспективы // УСиМ. – 2008. – №4. – С. 88-92.

3. Сумина Г.А., Кожанов Е.А., Степина А.Н. Защита информации в беспроводных сетях // Телематика-2008: труды XV Всероссийской научно-метод. конф., Санкт-Петербург, 23-26 июня 2008 г. – СПб, 2008. – С. 187-188.

4. Юдін О. К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних. – К.: Вид. «Інтерсервіс», 2009. – 716 с.

5. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / Под ред. В.Ф.Шаньгина. – М.: Радио и связь, 1999. – 328 с.

6. Печурин Н.К., Кондратова Л.П., Печурин С.Н. Применение инструментария формальных грамматик для переклассификации функций эталонной модели взаимодействия открытых систем в беспроводной компьютерной сети // Проблеми інформатизації та управління: зб. наук. праць. – 2012. – Вип. 2 (38). – С. 19-26.

7. Капітонова Ю.В., Кривий С.Л., Летичевський О.А., Луцький Г.М., Печурін М.К. Основи дискретної математики: Підручник. Т.2. - К.: Вид. «Літсофт», 2000. – 370 с.

Статью представлено в редакцию 7.11.2014