УДК 510.645:004.032.26

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

ИНСТРУМЕНТАРИЙ ФОРМАЛЬНЫХ ГРАММАТИК ДЛЯ ОБЕСПЕЧЕНИЯ МЕЖУРОВНЕВОГО БЕЗОПАСНОГО ВЗАИМОДЕЙСТВИЯ В БЕСПРОВОДНОЙ КОМПЬЮТЕРНОЙ СЕТИ ТИПА DSSS НА ОСНОВЕ ЭТАЛОННОЙ МОДЕЛИ

**[1]Институт компьютерных информационных технологий
Национального авиационного университета
[2]УНК «Институт прикладного системного анализа»
Национального технического университета Украины «КПИ»**

Инструментарий формальных грамматик предлагается применить для описания преобразований модулей данных с учетом функций защиты в эталонной модели. Предлагаемая модель трансляции модулей данных на основе предложений контекстно-свободной грамматики обеспечивает адекватное представление межуровневого преобразования для безопасного взаимодействия в процессе перехода между иерархическими уровнями эталонной модели

Введение

Защита информации представляет одну из наиболее приоритетных государственных задач в современных условиях непрерывного развития и продвижения на рынке беспроводных услуг. Конфиденциальность и целостность информации в беспроводных сетях стандартов IEEE 802.11, IEEE 802.16-2001, IEEE 802.16e-2005 обеспечивают средства физического уровня, идентификации набора служб, управления доступом к среде передачи, механизмы *WEP* и *WPA* аутентификации и шифрования с использованием соответственно статических и динамических ключей [1, 2]. В военной связи безопасность передачи обеспечивается применением технологии *DSSS* с модуляцией по схеме *CCK* ключей дополнительного кода для преобразования данных. Предложенный в [3] метод предусматривает введение в беспроводных сетях дополнительного уровня как модификацию сетевого уровня для реализации функции защиты информации, а также применение любого алгоритма шифрования. Как средство для установления связей между функциями эталонной модели (ЭМ) и точной ориентировки в их многообразии, рассмотренный в работе [4] подход к кластеризации функций ЭМ с применением инструментария сетей типа RBF и MLP выявил отличное от существующего в классической ЭМ распределение состава функций между иерархическими уровнями. В работе [5] предложена модель трансляции как адекватного межуровневого преобразования данных предложениями контекстно-свободной грамматики (КС-грамматики) с целью переклассификации функций ЭМ.

Целью данной статьи является развитие подхода, предложенного в [5], для межуровневого преобразования модулей данных с учетом функции защиты в ЭМ.

Постановка задачи

Известно множество $X_0 = \bigcup_{i=1}^{n} X_i$ (n - число уровней ЭМ ВОС) параметров распределённых по уровням ЭМ функций преобразования данных в составе с параметрами функций обеспечения целостности данных, шифрования и аутентификации. Функции преобразования модулей данных (*PDU*) реализуют также процедуры инкапсуляции и деинкапсуляции соответственно на передающей и принимающей станциях, формируя вложенные заголовки при добавлении к информации от выше расположенных уровней собствен-

ного заголовка. В беспроводной сети с технологией *DSSS* на подуровне *PLCP* физического уровня протокольные адреса преобразуются в эквивалентные им аппаратные адреса, содержащиеся в формате инкапсулируемого в аппаратном фрейме сообщения протокола ARP преобразования адресов набора протоколов TCP/IP [6, 7]. Параметры функций обеспечения защиты информации представлены в заголовке фрейма *PDU* подуровня *PLCP* и в заголовке *MAC*-фрейма, где указываются схема кодирования (поле *Service*) и технология шифрования (*WEP, WPA, WPA2*). Технологии *WPA, WPA2* отличаются использованием усовершенствованного протокола шифрования с динамическими ключами и криптографической контрольной суммой, подтверждающей целостность информации (контрольная сумма представляется функцией адреса источника, адреса назначения и поля данных). Предусмотренные стандартами 802.11 функции аутентификации в основе протокола EAP, отличающегося простотой реализации в аутентификаторе (точке доступа), выполняются с предварительным туннелированием, защищая от атак типа «man-in-middle», «session hihacking». Структуру *MAC*-фрейма представляют заголовок, данные и трейлер. В заголовке с общей длиной 24 – 2340 байт в поле контроля фрейма длиной 2 байта содержится параметр, характеризующий технологию шифрования. На рис.1 представлен формат фрейма *PDU* подуровня *PLCP* с вложенным *MAC*-фреймом в структуре фрейма *PPDU*.

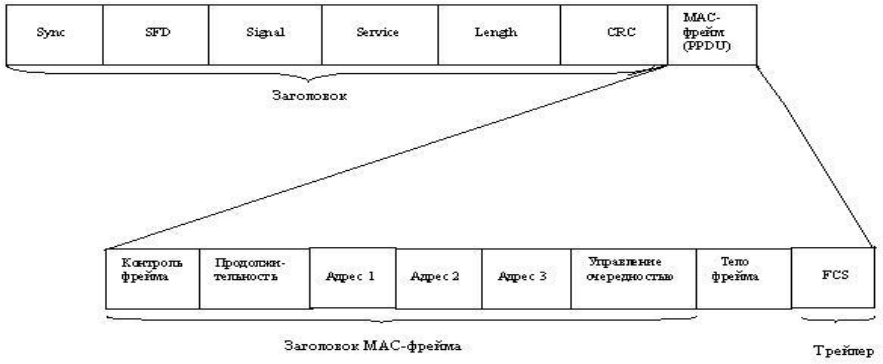

Рис. 1. Формат фрейма подуровня *PLCP* для метода передачи *DSSS*

с вложенным фреймом *MAC*-уровня.

Заголовок в формате фрейма (см. рис.1) включает поля преамбулы, предназначенные для обеспечения синхронизации в приемной станции пакетов (*Sync* со строкой, состоящей из единиц, с максимальным размером 128 бит) и фреймов (*SFD* со строкой 1111 0011 1010 0000 для длинного формата и 0000 0101 1100 1111 для короткого формата). Результат инкапсуляции данных и заголовка представляют 2 вложенных заголовка в структуре фрейма подуровня *PLCP*.

Модель трансляции фрейма

Модель трансляции фрейма *PPDU* со структурой на рис.1 представляет множество правил продукций метаязыка ЭМ с КС-грамматикой $G = \langle V_T, V_H, s, P \rangle$, где $V_T = \{0,1, A, B, C, D, ..., LH, FCS\}$ - алфавит терминальных символов с обозначениями LH для задаваемых параметров в заголовках фрейма, FCS для контрольной суммы и множествами $\{0,1\}$ и $\{A, B, C, D, ...\}$, используемыми при формировании последовательностей битов

заголовков и тела фрейма; $V_H = \{PPDU, \text{ÇÀÃÎËÎÂÎÊ}, \text{ÄÀÍÍÛÅ}, \text{ÒÐÅÉËÅÐ}, SS\}$ - вспомогательный алфавит нетерминальных символов (метапеременные, используемые в левой части правил множества P); SS - вспомогательная метапеременная, введенная для формирования заголовка; $s = PPDU \in V_H$ - начальный нетерминальный символ; P - множество правил продукций типа $x \to v$, где $x \in V_H, , v \in F(V)$, $F(V)$ – свободная полугруппа слов над алфавитом $V = V_T \cup V_H$ [8]. В системе правил будем использовать обозначение e для пустой цепочки. Множество P представляет систему следующих правил:

$$PPDU \to \text{ÇÀÃÎËÎÂÎÊ} \; PPDU \mid \text{ÇÀÃÎËÎÂÎÊ} \; \text{ÄÀÍÍÛÅ} \; \text{ÒÐÅÉËÅÐ}; \tag{1}$$

$$\text{ÇÀÃÎËÎÂÎÊ} \to SS \; LH \; FCS \mid SS \; LH; \tag{2}$$

$$SS \to 0\,SS\,1 \mid 0\,SS \mid 1\,SS \mid e; \tag{3}$$

$$\text{ÄÀÍÍÛÅ} \to A \mid B \mid C \ldots; \quad \text{ÒÐÅÉËÅÐ} \to FCS. \tag{4}$$

Формирование последовательности битов модуля PPDU

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:

$$\underbrace{11\ldots1}_{128}1111001110\,1000000011\,0111000000\,LHFCS,$$

$$\underbrace{11\ldots1}_{56}0000\,0101110011110011011100000\,0LHFCS \tag{5}$$

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

$$\underbrace{11\ldots1}_{128}1111001110\,1000000110\,1110000000\,LHFCS,$$

$$\underbrace{11\ldots1}_{56}0000\,010111001111011011100000000\,LHFCS. \tag{6}$$

Цепочки терминалов (5), (6) 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.

Выводы

Описанный инструментарий формальных грамматик предназначен для описания преобразований модулей данных с учетом функций обеспечения целостности информации в беспроводной

компьютерной сети с технологией DSSS в процессе межуровневого взаимодействия на основе эталонной модели. С применением предлагаемой модели трансляции модулей данных на основе предложений контекстно-свободной грамматики получено адекватное представление последовательности битов, характеризующей безопасное межуровневое взаимодействие в процессе перехода между иерархическими уровнями эталонной модели.

Список литературы

1. Иманкул М.Н. Защита беспроводной компьютерной сети // Вестник ЕНУ им. Л.Н.Гумилева. – 2011. - №6. – С.39-46.

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. Печурин Н.К., Кондратова Л.П., Печурин С.Н. Подход к кластерному анализу функций эталонной модели взаимодействия открытых систем с применением инструментария прямонаправленных искусственных нейронных сетей // Проблеми інформатизації та управління: зб. наук. праць.–2012. – Вип. 3 (39). – С. 36-43.

5. 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.

6. Дуглас Э.Камер. Компьютерные сети и Internet. Разработка приложений для Internet. – М.: Издательский дом «Вильямс». - 2002. – 640 с.

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

8. Капитонова Ю.В., Кривой С.Л., Летичевский А.А., Луцкий Г.М. Лекции по дискретной математике. - СПб.: БХВ-Петербург, 2004. – 624 с.

Статтю подано до редакції 16.12.2013