УДК 510.645:004.032.26

И.А. Жуков[1], **Н.К. Печурин**[1], доктора техн. наук,
Л.П. Кондратова[2], **С.Н. Печурин**[1], кандидаты техн. наук
[1] Ин-т компьютерных информационных технологий НАУ
(Украина, 03058, Киев, пр-т Комарова, 1,
тел.(+38) 0683220610, e-mail: pechnk@mail.ru),
[2] УНК «Ин-т прикладного системного анализа» НТУУ «КПИ»
(Украина, 03056, Киев, пр-т Победы, 37,
тел. (+38) 0973596517, e-mail: ljupav@yandex.ua)

Представление взаимодействия уровней компьютерной сети *DSSS* и *FHSS* моделью регулярных языков и грамматик

Предложено применить модели регулярных языков и грамматик для описания преобразований протокольных модулей данных на физическом и канальном уровнях эталонной модели взаимодействия открытых систем. Предлагаемый способ описания трансляции модулей основан на инструментарии регулярных грамматик и обеспечивает адекватное представление межуровневого преобразования в процессе перехода между нижними иерархическими уровнями эталонной модели.

Запропоновано застосувати моделі регулярних мов і граматик для опису перетворень протокольних модулей даних на фізичному і канальному рівнях еталонної моделі взаємодії відкритих систем. Даний спосіб опису трансляції модулей оснований на інструментарії регулярних граматик і забезпечує адекватне представлення міжрівневого перетворення у процесі переходу між нижніми ієрархічними рівнями еталонної моделі.

К л ю ч е в ы е с л о в а: модель, регулярные языки и грамматики, протокольный модуль данных, беспроводная компьютерная сеть.

Базовые методы доступа в беспроводных компьютерных сетях, называемые также методами уплотнения или мультиплексирования, основаны на разделении между станциями таких параметров, как пространство, время, частота и код. Задача уплотнения — выделить каждому каналу связи пространство, время, частоту и (или) код с минимумом взаимных помех и максимальным использованием характеристик передающей среды. 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].

Предложенный в [2] 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 [3] 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 [4] предложена модель трансляции как адекватного межуровневого преобразования данных предложениями контекстно-свободной грамматики (КС-грамматики) с целью переклассификации функций ЭМ.

Предлагаемый подход, являющийся развитием подхода, описанного в [4], предназначен для адекватного представления межуровневого взаимодействия в беспроводной компьютерной сети протокольных модулей данных канального и физического уровня.

Постановка задачи. Известно множество $X_0 = \bigcup_{i=1}^{n} X_i$ (n — число уровней ЭМ взаимодействия открытых систем) параметров распределенных по уровням ЭМ функций преобразования данных в составе параметров 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 собственного заголовка. В беспроводной сети, использующей технологии *FHSS* и *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 [5, 6].

Параметры функций обеспечения защиты информации, представленные в заголовке фрейма *PDU* подуровня *PLCP* и в заголовке *MAC*-фрейма, указывают предусмотренные технологией *DSSS* схему кодирования (поле *Сигнал*) и технологию шифрования (*WEP*, *WPA*, *WPA*2). В технологиях *WPA*, *WPA*2 используется усовершенствованный протокол шифрования с динамическими ключами и криптографической контрольной суммой, подтверждающей целостность информации (контрольная сумма как функция

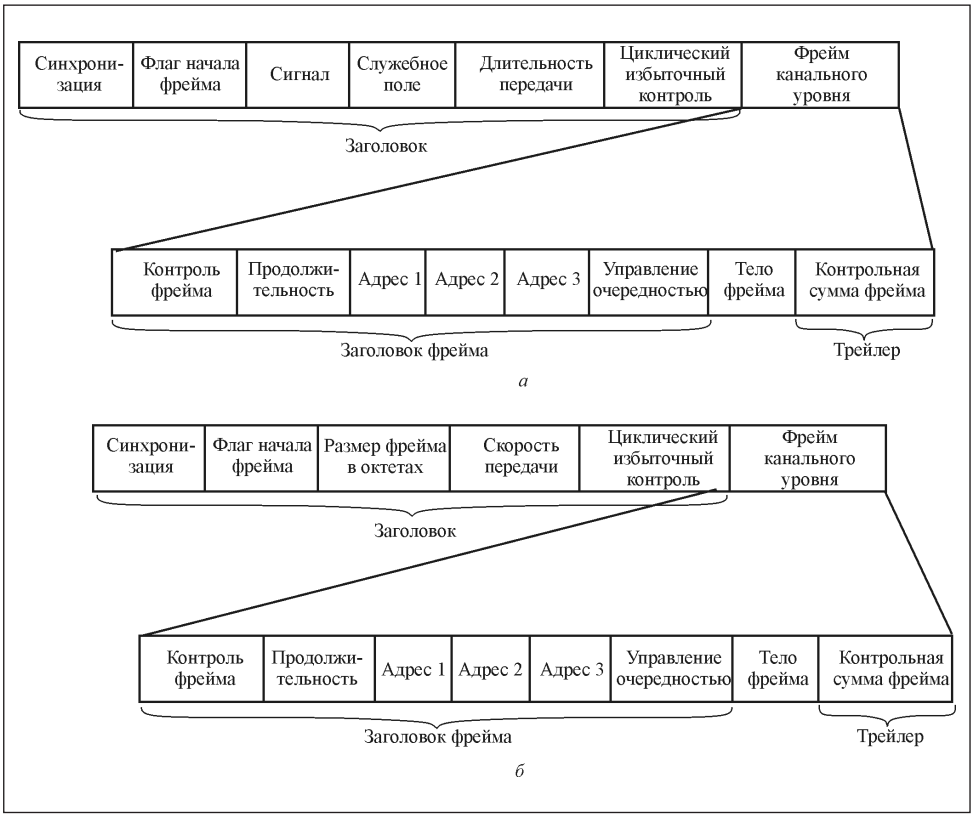

Рис. 1. Форматы фрейма подуровня *PLCP* с вложенным фреймом канального уровня: *а* — метод передачи *DSSS*; *б* — метод передачи *FHSS*

адреса источника, адреса назначения и поля данных представляет результат обнаружения всех одиночных ошибок, двойных ошибок и ошибок в нечетном числе битов).

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 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* для компьютерной сети с технологиями *DSSS* и *FHSS*. Заголовок в формате фрейма включает поля преамбулы, предназначенные для обеспечения синхронизации в приемной станции пакетов (поля синхронизации размером 128 бит для *DSSS* со стро-

кой, состоящей из единиц, и размером 80 бит со строкой, состоящей из чередующихся 0 и 1 для *FHSS*) и фреймов (*SFD* со строкой 1111 0011 1010 0000 для длинного формата и 0000 0101 1100 1111 для короткого формата — обратной по отношению к длинному заголовку в *DSSS* и *SFD* со строкой 0000 1100 1011 1101 в *FHSS*). Результат инкапсуляции данных и заголовка представляют два вложенных заголовка в структуре фрейма подуровня *PLCP*.

Модель представления межуровневого взаимодействия в беспроводной компьютерной сети. Межуровневое взаимодействие в беспроводной компьютерной сети описывается моделью трансляции фреймов *PPDU*, используемых в технологиях *DSSS* и *FHSS* (см. рис. 1). В модели представлено множество леволинейных и праволинейных правил продукций метаязыка ЭМ с регулярной грамматикой $G=(V_T, V_H, \sigma, P)$. Здесь $V_T=\{0, 1, A, B, C, D, ..., LH, FCS\}$ — алфавит терминальных символов с обозначениями *LH* для задаваемых параметров в заголовках фрейма и *FCS* — для контрольной суммы; $\{0,1\}$ и $\{A, B, C, D, ...\}$ — множества, используемые при формировании последовательностей битов заголовков и тела фрейма; $V_H=\{PPDU, ЗАГОЛОВОК, ДАННЫЕ, ТРЕЙЛЕР, P, SS\}$ — вспомогательный алфавит нетерминальных символов (метапеременные, используемые в левой части правил множества *P*); *SS* — вспомогательная метапеременная, введенная для формирования заголовка; $\sigma = PPDU \in V_H$ — начальный нетерминальный символ; *P* — множество правил продукций типа $\xi \to v$, где $\xi \in V_H$; $v \in F(V)$, $F(V)$ — свободная полугруппа слов над алфавитом $V = V_T \cup V_H$ [7, 8].

В системе правил будем использовать обозначение ε для пустой цепочки. Множество *P* представляет систему следующих праволинейных и леволинейных правил:

$$PPDU \to ЗАГОЛОВОК\ PPDU \mid ЗАГОЛОВОК\ ДАННЫЕ\ ТРЕЙЛЕР, \quad (1)$$

$$ЗАГОЛОВОК \to SSLHFCS \mid SSLH, \quad (2)$$

$$SS \to 0SS1 \mid 0SS \mid 1SS \mid \varepsilon, \quad (3)$$

$$ДАННЫЕ \to A \mid B \mid C ...; ТРЕЙЛЕР \to FCS. \quad (4)$$

Процедура трансляции фрейма. Рассмотрим модуль *PPDU*, используемый в технологии *DSSS*. Преобразование фрейма в последовательность битов выполняется с использованием схемы кодирования с дополнительными кодами (ССК) 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, имеют соответственно вид

$$\underbrace{11\ldots1}_{128}1111001110\ \ 1000000011\ 0111000000\ \ LHFCS\ \ ,$$
$$\underbrace{11\ldots1}_{56}0000\ \ 01011100\ 1111001101\ 11000000LH\ \ \ FCS. \tag{5}$$

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

$$\underbrace{11\ldots1}_{128}1111001110\ \ 1000000110\ 1110000000\ \ LHFCS,$$
$$\underbrace{11\ldots1}_{56}0000\ \ 0101\ 1100\ 1111011011\ 10000000LH\ \ \ FCS. \tag{6}$$

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 единице параметр, определяющий механизм *WEP* шифрования.

Таким образом, процесс преобразования информации в направлении от надприкладного (смыслового) уровня к физическому, через *DSSS* и *FHSS*, представляется моделью порождения предложений регулярного (контекстно-свободного) языка по продукционным правилам, описанным выше. Процесс обратного перехода, от физического уровня к прикладному на приемной стороне, представляется моделью грамматического разбора полученных предложений.

Разбор предложения, полученного на физическом уровне, т.е. поиск корня дерева грамматического разбора, по сути является процессом обратного отображения (функции) информации надприкладного уровня в предложения физического уровня. Вследствие наличия большого числа степеней свободы при поиске корня дерева грамматического разбора (рис. 2) процедура поиска приобретает черты поиска аргумента однонаправленной функции. Это обстоятельство, с точки зрения защиты, позволяет рассматривать систему преобразования информации «надприкладной (смысловой) уровень — прикладной — … — физический — передача данных —

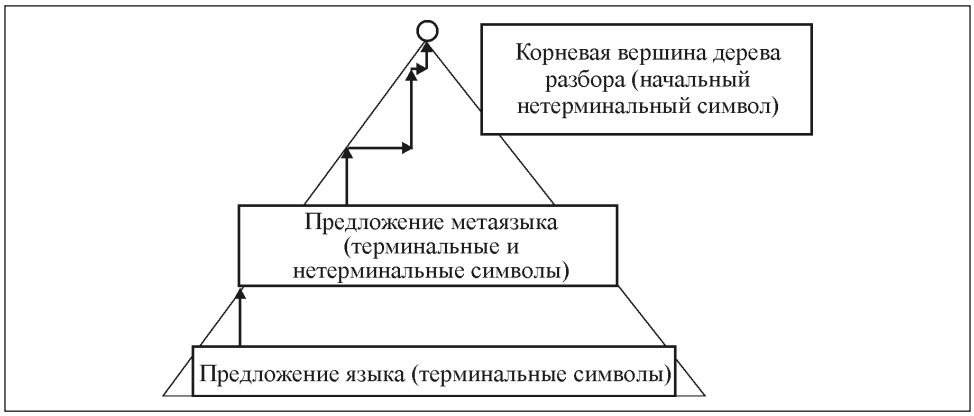

Рис. 2. Одна из стратегий грамматического разбора предложения физического уровня

физический — канальный — … — прикладной — надприкладной (смысловой)» как асимметричную криптосистему [9].

Выводы

Предлагаемый способ описания трансляции модулей основан на инструментарии регулярных грамматик и обеспечивает адекватное представление межуровневого преобразования в процессе перехода между нижними иерархическими уровнями эталонной модели с учетом функций обеспечения целостности информации в беспроводной компьютерной сети. Применение предлагаемой модели трансляции протокольных модулей данных на основе предложений грамматики с леволинейными и праволинейными правилами позволяет получить адекватное представление последовательности битов, характеризующей безопасное межуровневое взаимодействие в процессе перехода между иерархическими уровнями эталонной модели для компьютерной сети с технологией *DSSS*.

С помощью предложенной модели однонаправленного отображения могут быть построены алгоритмы асимметричных криптографических систем.

It is proposed to use the models of regular languages and grammars to describe the protocol data units transformations at the physical and data link levels of the open systems interconnection reference model. The proposed way to describe the modules' translation is based on the regular grammars tools and ensures the adequate representation of the inter-layer transformation in the transition between the lower hierarchical levels of the reference model.

СПИСОК ЛИТЕРАТУРЫ

1. *Лисецкий Ю.М., Бобров С.И.* WiMAX сети. Реализации и перспективы // УСиМ. — 2008. — № 4. — С. 88—92.
2. *Сумина Г.А., Кожанов Е.А., Степина А.Н.* Защита информации в беспроводных сетях // Телематика-2008. Тр. XV Всероссийской науч.-метод.конф. Санкт-Петербург, 23—26 июня 2008 г. — СПб, 2008. — С. 187—188.
3. *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.
4. *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 // Там же. — 2012. — Вип. 2 (38). — С. 19—26.
5. *Дуглас Э. Камер.* Компьютерные сети и Internet. Разработка приложений для Internet. — М. : Изд. дом «Вильямс», — 2002. — 640 с.
6. *Рошан П., Лиэри Дж.* Основы построения беспроводных локальных сетей стандарта 802.11. — М. : Изд. дом «Вильямс», 2004. — 304 с.
7. *Капітонова Ю.В., Кривий С.Л., Летичевський А.А. та ін.* Основи дискретної математики. — Київ. : Наук. думка, 2002. — 579 с.
8. *Жабин В.И., Жуков И.А., Клименко И.А., Ткаченко В.В.* Прикладная теория цифровых автоматов. — Киев : Изд. НАУ, 2007. — 364 с.
9. *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.

Поступила 26.12.13

ЖУКОВ Игорь Анатольевич, д-р техн. наук, профессор, зав. кафедрой компьютерных систем и сетей Ин-та компьютерных технологий Национального авиационного университета Украины. В 1974 г. окончил Киевский ин-т инженеров гражданской авиации. Область научных исследований — анализ и синтез структуры компьютерных информационных систем.

ПЕЧУРИН Николай Капитонович, д-р техн. наук, профессор, профессор кафедры компьютерных систем и сетей Ин-та компьютерных технологий Национального авиационного университета Украины. В 1973 г. окончил Киевский политехнический ин-т. Область научных исследований — системный анализ и информационно-телекоммуникационные технологии, моделирование компьютерных сетей.

КОНДРАТОВА Людмила Павловна, канд. техн. наук, ст. науч. сотр. Учебно-научного комплекса «Ин-т прикладного системного анализа» Национального технического университета Украины «Киевский политехнический ин-т». В 1976 г. окончила Киевский политехнический ин-т. Область научных исследований — системный анализ и информационные технологии, моделирование компьютерных сетей.

ПЕЧУРИН Сергей Николаевич, канд. техн. наук, ассистент кафедры компьютерных систем и сетей Ин-та компьютерных технологий Национального авиационного университета Украины. В 1996 г. окончил Национальный технический университет Украины «Киевский политехнический ин-т». Область научных исследований — системный анализ и информационные технологии, моделирование компьютерных сетей.