— IEEE 802.11i (Draft 3), в котором предлагается протокол WPA, использующий контроль целостности сообщений, генерацию динамических ключей шифрования, а также увеличенные длины векторов инициализации алгоритма RC4. Сегодня также известны уязвимости в данном протоколе;
— IEEE 802.11i (WPA2, 2004 г.). Его механизмы являются наиболее безопасным решением на сегодняшний день, для шифрования трафика используется алгоритм AES.

В процессе исследования проводилось пассивное сканирование эфира при помощи свободно распространяемых утилит (Kismet, airodump-ng). Основные выводы делались на основе служебных фреймов Beacon и Probe Response. Передаваемые в сетях данные, а также координаты точек доступа не сохранялись. Была собрана информация по следующим показателям:

— используемые механизмы шифрования (WEP, WPA, WPA2 или никакой);
— рассылка идентификатора сети;
— использование настроек по умолчанию;
— производители оборудования;
— состав сетей (количество точек доступа);
— стандарты передачи данных (частотный диапазон, скорость передачи, радиус действия);
— загруженность частотных каналов.

На основе собранных материалов получены следующие данные о защищенности беспроводных сетей г. Томска:

— 71 % сетей используют шифрование, однако в большинстве используются механизмы WEP и WPA, которые в той или иной степени могут быть скомпрометированы;
— большая часть сетей представлена лишь одной точкой доступа, что говорит об активном использовании беспроводных технологий частными лицами;
— для 8 % сетей не удалось определить производителя оборудования, что может быть связано с ручным изменением параметров оборудования;
— добровольная рассылка идентификатора сети включена в 88 % сетей, из них 22 % используют идентификатор по умолчанию.

Сравнение полученных результатов с результатами аналогичных исследований в других городах (см., например, [1 – 3]) показало, что общая ситуация в Томске соотносится с общемировыми показателями.

ЛИТЕРАТУРА

1. http://www.securitylab.ru/analytics/270874.php
2. http://www.securelist.com/ru/analysis?pubid=204007548
3. http://www.securelist.com/ru/analysis/204007540/Wardriving_v_Varshave

УДК 004.773.5

МЕТОД ЗАЩИТЫ ЦИФРОВОЙ ВИДЕОИНФОРМАЦИИ ПРИ ЕЁ ПЕРЕДАЧЕ В РАСПРЕДЕЛЕННЫХ КОМПЬЮТЕРНЫХ СЕТЯХ

Е. В. Щерба

Неотъемлемым атрибутом большинства видеосистем становится использование потоковой передачи видеоинформации по компьютерным сетям. Но при передаче информации по открытому каналу связи неизбежно встает задача её защиты. Наиболее часто

для решения этой задачи используется шифрование передаваемых данных. Но большинство традиционных систем шифрования не могут напрямую использоваться для работы с потоковой видеоинформацией [1]. Альтернативным решением задачи защиты передаваемой информации может служить система мультиплексирования трафика [2].

Такая модель (рис. 1), по сути, является схемой разделения секрета, участниками которой являются промежуточные узлы сети, а в роли проекций выступают производные части исходных данных, полученные в результате сегментирования. В качестве единицы исходных данных, подлежащих сегментированию, естественным образом выступает кадр видеопотока. В основе любого алгоритма сегментирования лежит принцип разбиения множества всех точек изображения на некоторое количество непересекающихся классов. Задачей в данном случае является поиск такого способа разбиения, при котором практическая ценность перехваченной аналитиком информации была бы минимальной. Основной подход к решению данной задачи заключается в восстановлении исходного изображения на основе некоторого (неполного) числа проекций методами интерполяции и экстраполяции [3].

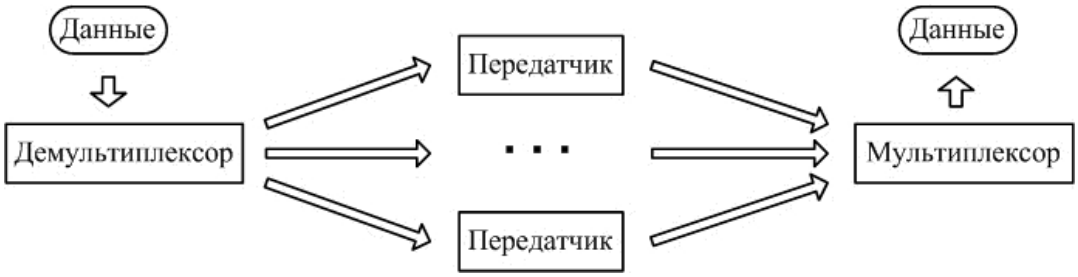

Рис. 1. Модель системы мультиплексирования трафика

Целью восстановления изображения $h(x, y)$, скомпонованного из проекций, является получение из него при помощи некоторой обработки изображения $\widehat{f}(x, y)$, которое близко к идеальному изображению $f(x, y)$ по заданному критерию. В результате проведенных исследований был предложен способ образования проекций на основе значения $f(x, y)$. Каждая проекция в результате сегментирования будет включать в себя точки из определенного диапазона яркости, число которых определяется числом проекций. В схеме с двумя проекциями эти классы задаются следующим образом:

$$P_0 = \left\{ (x,y) \left| f(x,y) \leqslant \frac{1}{M_1 M_2} \sum_{x=0}^{M_1-1} \sum_{y=0}^{M_2-1} f(x,y) \right. \right\},$$

$$P_1 = \left\{ (x,y) \left| f(x,y) > \frac{1}{M_1 M_2} \sum_{x=0}^{M_1-1} \sum_{y=0}^{M_2-1} f(x,y) \right. \right\}.$$

А для случая произвольного числа $n = 2^k$ $(k > 1)$ проекций определение классов происходит рекуррентно:

$$P_i = \left\{ (x,y) \left| f(x,y) \leqslant \frac{2^{k-1}}{M_1 M_2} \sum_{(x,y) \in \overline{P}_j} f(x,y) \right. \right\},$$

$$P_{i+1} = \left\{ (x,y) \left| f(x,y) > \frac{2^{k-1}}{M_1 M_2} \sum_{(x,y)\in\overline{P}_j} f(x,y) \right. \right\}.$$

Здесь $\overline{P}_j$ — это класс, полученный для схемы с 2^{k-1} проекциями, т. е. $j \in \left[0; 2^{k-1}\right]$, а $i = 2j$. Поскольку при переходе точки из изображения в проекцию её координаты сохраняются, некоторое количество точек в проекции будет не определено, т. е. будут образованы «яркостные» разрывы. Особенность разрывов такого рода состоит в том, что применяемое для них «сглаживание» не обеспечивает необходимого результата, а дисперсия ошибки интерполяции с увеличением числа проекций в системе растет быстрее, чем для случайного разрыва. Кроме того, поскольку выборка данных в проекцию не случайна, возможность линейного прогнозирования отсутствующих данных также исключена.

Представленный метод реализован в качестве фильтра Microsoft DirectShow, предназначенного для преобразования кадра исходного видеопотока в проекцию производного видеопотока с помощью яркостного метода сегментирования.

ЛИТЕРАТУРА

1. *Володин А. А., Митько В. Г., Спинко Е. Н.* Метод защиты канала передачи видеоинформации на основе мультиплексирования трафика // Вопросы защиты информации. 2002. С. 34–47.
2. *Щерба Е. В.* Метод защиты канала передачи видеоинформации на основе мультиплексирования трафика // Вопросы защиты информации. 2008. № 1(80). С. 55–60.
3. *Гонсалес Р., Вудс Р.* Цифровая обработка изображений. М.: Техносфера, 2005. 1072 с.