После выбора на двух кадрах групп подходящих точек, требуется определить соответствие между ними. Это может быть сделано с помощью кросс-корреляции, которая служит мерой подобия участков изображения. Циклическая кросс-корреляция может быть вычислена через преобразование Фурье согласно теореме о свертке [4]:

$$F(f_1(x,y) \otimes f_2(x,y)) = F(f_1(x,y)) \cdot F^*(f_2(x,y)), \qquad (5)$$

где F – преобразование Фурье, * – комплексное сопряжение.

Для оценки подобия участков изображения, кросс-корреляцию следует нормировать относительно корня из произведения максимумов автокорреляционных функций участков.

Обладая сопоставленными координатами точки на нескольких кадрах, не сложно определить координаты ее положения в пространстве $\mathbf{P}$, используя известные проекционные матрицы кадров $\mathbf{M}_i$ [1]:

$$\begin{cases} \mathbf{p}_1 \times \mathbf{M}_1\mathbf{P} = 0 \\ \dots \\ \mathbf{p}_n \times \mathbf{M}_n\mathbf{P} = 0 \end{cases}, \qquad (6)$$

Данная система очевидно является избыточной при любом количестве кадров, большим одного. Поэтому, в общем случае из-за неточности определения координат проекций $\mathbf{p}_i$, она не будет иметь решения. Поэтому на практике используют приближенное решение данной системы, которое можно найти, например [1], с помощью схемы наименьших квадратов для отклонений координат проекции искомой точки на фоточувствительную матрицу от координат, полученных из анализа кадров.

Литература

1. *Forsyth D., Ponce J.* Computer Vision: a modern approach, Pearson Education, 2003.
2. *Press W. H., Teukolsky S. A., Vetterling W. T., Flannery B. P.* Numerical recipes in C: the art of scientific computing. Cambridge University Press, 1992.
3. *Сойфер В. А.* Методы компьютерной обработки изображений. М., 2003.
4. *Shapiro L., Stockman G.* Computer vision. Prentice Hall, 2001.

ИСПОЛЬЗОВАНИЕ RFID-МЕТОК ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ СЕТЕЙ

Ю. Ю. Литвинович, П. П. Мягков

ВВЕДЕНИЕ

В настоящее время все большее распространение получают беспроводные сети. Их используют для широкого круга задач, таких как созда-

ние локальной сети, соединение устройств напрямую и, конечно, выхода в интернет.

Беспроводные устройства связываются друг с другом, используя в качестве переносчика данных сигналы, передаваемые в определенном диапазоне радиочастот. Недостатком такого механизма является то, что любая другая станция, использующая этот диапазон, также способна принять эти данные.

В связи с этим очень актуальна проблема защиты информации в беспроводных сетях от несанкционированного доступа.

Каждый стандарт беспроводных сетей имеет свои особенности и методы защиты. Однако они все не лишены уязвимостей. Например, в сетях Wi-Fi стандарта 802.11 используются технологии защиты WEP и WPA/ WPA2. Проведенное нами исследование показало, что с помощью существующих методик атак WEP взламывается за считанные секунды, а взлом WPA/WPA2 возможен, и при определенных условиях (малая длина ключа, использование простых паролей и др.) вполне прост.

В данной статье предлагается вариант решения этой проблемы – использование RFID-меток для обеспечения безопасного доступа к беспроводной сети.

RFID (англ. “Radio Frequency Identification”, радиочастотная идентификация) – метод автоматической идентификации объектов, в котором посредством радиосигналов считываются или записываются данные, хранящиеся в так называемых RFID-метках.

Любая RFID-система состоит из считывающего устройства (считыватель или ридер) и транспондера (он же RFID-метка).

Большинство RFID-меток состоит из двух частей. Первая – интегральная схема (ИС) для хранения и обработки информации, модулирования и демодулирования радиочастотного (RF) сигнала и некоторых других функций. Вторая – антенна для приёма и передачи сигнала.

RFID-метки широко используются в промышленности, производстве продовольствия, логистике, медицине [3]. Еще одним возможным применением RFID-технологии может служить обеспечение безопасности беспроводных сетей.

УЯЗВИМОСТИ СУЩЕСТВУЮЩИХ МЕТОДОВ ЗАЩИТЫ

Для обеспечения хотя бы минимального уровня безопасности беспроводных сетей необходимы следующие компоненты [1]:

1. **Контроль доступа**. Необходим для принятия решения относительно того, кто или что может использовать беспроводную сеть. Для сетей стандарта 802.11 это требование удовлетворяется за счет механиз-

ма аутентификации, скрытия SSID сети, фильтрации по MAC-адресам, уменьшения дальности действия точки.

2. **Средства шифрования** – средства защиты информации, передаваемой через беспроводную среду. Это требование удовлетворяется за счет использования технологий шифрования (WEP, WPA, WPA2 и др.).

В ходе анализа защищенности вышеприведенных компонент были установлены следующие уязвимости.

При открытой аутентификации (open authentication) любой пользователь может получить доступ в сеть, а при знании секретного ключа, доступ в сеть обеспечен и при аутентификация с совместно используемым ключом (shared key authentication).

Скрытие SSID сети может быть легко взломано ввиду того, что SSID можно заполучить путем прослушивания трафика (traffic sniffing**)**, т.к. он передается в незашифрованном виде.

Фильтрация по MAC-адресам также имеет уязвимости, потому что дозволенные MAC-адреса, передающиеся в незашифрованном виде, можно заполучить путем сниффинга и присвоить их своей сетевой карте.

В шифровании передаваемых данных уязвимости были обнаружены в механизме шифрования WEP, а именно в применяющемся там поточном шифре RC4. Часть векторов инициализации (их называют слабые Initialization Vectors – weak IV) могут раскрыть биты ключа в результате проведения статистического анализа даже без методов брутфорса (англ. “brute force”, грубая сила). Также существует уязвимость в контрольном признаке целостности (ICV). ICV (Integrity Check Value) базируется на полиномиальной функции CRC-32. Математические свойства функции CRC-32 позволяют подделать фрейм и модифицировать значение ICV, даже если исходное содержимое фрейма неизвестно. Это открывает дорогу к атакам с использованием побитовой обработки (или "жонглирования битами", bit flipping) [2].

ЗАЩИТА БЕСПРОВОДНЫХ СЕТЕЙ С ПОМОЩЬЮ RFID

Предлагаемым вариантом защиты беспроводных сетей является применение RFID-меток для получения доступа в сеть. Идею использования можно описать так: доступ в сеть получают только те устройства, которые знают идентификационные данные для входа в сеть (логин и пароль) и имеют уникальную RFID-метку, которая находится в списке «легальных» для данной сети. Сеть предоставляет доступ только при наличии всех 3-х компонент: логина, пароля и RFID-метки, которая физически существует только в одном экземпляре для конкретного пользователя.

Основным преимуществом использования RFID-меток, наряду с логическим уровнем защиты, является задействование и физического уровня, который намного более стойкий к взлому и имеет намного меньший процент уязвимостей.

Ниже приведена возможная схема применения описанной выше идеи для провайдеров, предоставляющих доступ к сети Интернет по беспроводной технологии.

Провайдер вместе с уникальным логином и паролем выдает клиенту также уникальную RFID-метку и USB-считыватель. RFID-метка может быть сделана в виде пластинки произвольной формы и размеров (например, кредитной карточки), в виде SIM-карточки или брелока.

При входе в сеть на первом этапе клиент использует свои логин и пароль для установления начального зашифрованного соединения. На втором этапе точка доступа запрашивает данные RFID-метки. Клиент использует выданные ему метку и считыватель для подтверждения своей личности. Данные с RFID-метки передаются уже в зашифрованном виде, что усложняет их кражу и подделку для несанкционированного использования. После успешного прохождения второго этапа аутентификации, ключи шифрования изменяются, генерируясь еще раз с использованием данных с RFID-метки.

Все это позволяет обеспечить надежный способ защиты соединения, который крайне труден для взлома из-за того, что используется комбинация как логической, так и физической защиты соединения.

Литература

1. *Мерритт М., Поллино Д.* Безопасность беспроводных сетей. М.: Академия АйТи, 2004.
2. *Fleishman G, Engst A.* Take Control of Your Wi-Fi Security. N.-Y.: TidBITS Publishing, 2009.
3. *Сандип Л.* RFID. Руководство по внедрению. М.: Кудиц-Пресс, 2007.

АДАПТИВНЫЕ ГИДРОАКУСТИЧЕСКИЕ АНТЕННЫЕ РЕШЕТКИ

С. И. Люзин

ВВЕДЕНИЕ

Основным элементом современных систем связи, локации, позиционирования и взаимной ориентации являются кольцевые фазированные антенные решетки (ФАР). Неконтролируемый разброс коэффициентов передачи элементов, обусловленный ошибками изготовления, приводит