«SecureTower» российской компании Falcongaze [1]. В качестве эксперимента 2 тестовых файла (формат: doc, rar; объем: до 50 КБ) с конфиденциальной информацией с использованием стенографического ПО «OpenPuff» (v.4.00 /настройки качества: по умолчанию/, LSB-метод) [2] встраивались в файл-контейнер (формат: png, jpg, pdf). Эффективность перехвата оценивалась в процентах от детекции сформированной тестовой базы из 6 файлов. Моделирование проводилось на физических и виртуальных вычислительных машинах (ПО «VMware Workstation Pro» [3]).

На основании проведенного исследования можно сделать вывод, что использование DLP-системы в настоящее время не позволяет детектировать стеганографические технологии модификации файлов. Эффективность перехвата данных DLP-системой по заданному перечню стеганографических модификаций файлов составила 0 % («цифровой отпечаток» (Digital Fingerprints) / контрольная сумма (хэш)).

Литература

1. Falcongaze «SecureTower» // falcongaze.ru [Электрон. ресурс]. – 2010-2017. – Режим доступа: https://falcongaze.ru/. – Дата доступа: 22.04.2017.

2. OpenPuff team // download.cnet.com [Электрон. ресурс]. – 2017. – Режим доступа: http://download.cnet.com/windows/openpuff-team/3260-20_4-10146585-1.html. – Дата доступа: 23.04.2017.

3. VMware Workstation Pro // vmware.com [Электрон. ресурс]. – 2017. – Режим доступа: http://www.vmware.com/ru/products/workstation.html. – Дата доступа: 22.04.2017.

ТЕСТИРОВАНИЕ ТЕХНОЛОГИЙ ПЕРЕХВАТА ДАННЫХ DLP-СИСТЕМЫ

В.В. Маликов, Е.О. Перхальский, И.И. Лившиц

Внедрение и использование DLP-систем позволяет эффективно автоматизировать ряд задач по защите конфиденциальной информации от утечки по технических каналам. Для оценки эффективности была выбрана DLP-система «SecureTower» российской компании Falcongaze [1], которая представляет собой программный продукт, позволяющий решать задачи по защите конфиденциальной информации от утечки по технических каналам.

В рамках исследования эффективности проведено:

Тестирование программной среды функционирования DLP-системы на предмет поддерживаемых операционных систем (ОС). Моделирование проводилось на физических и виртуальных вычислительных машинах (ПО «VMware Workstation Pro» [2]).

Тестирование эффективности перехвата данных DLP-системой в приложениях, использующих протоколы: POP3, SMTP, HTTP и др.). Назначение портов приложений использовались по умолчанию. Эффективность перехвата оценивалась в процентах от детекции сформированных тестовых баз из 20 файлов / сообщений в 2-х режимах DLP-системы (настройки по умолчанию / специальная настройка параметров). Моделирование проводилось на физических и виртуальных вычислительных машинах (ПО «VMware Workstation Pro»).

На основании проведенного исследования эффективности работы DLP-системы по защите конфиденциальной информации от утечки по технических каналам можно сделать следующие выводы:

1. Программная среда функционирования DLP-системы Falcongaze «SecureTower» в настоящее время поддерживает все основные ОС семейства Microsoft «Windows».

2. Внедрение и использование DLP-системы позволяет эффективно автоматизировать задачи по защите конфиденциальной информации от утечки по технических каналам. Эффективность перехвата данных DLP-системой по заданному перечню протоколов / портов составила от 90 % до 100 %.

Литература

1. Falcongaze «SecureTower» // falcongaze.ru [Электрон. ресурс]. – 2010-2017. – Режим доступа: https://falcongaze.ru/. – Дата доступа: 22.04.2017.

2. VMware Workstation Pro // vmware.com [Электрон. ресурс]. – 2017. – Режим доступа: http://www.vmware.com/ru/products/workstation.html. – Дата доступа: 22.04.2017.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СЕТЕЙ FANET

А.В. Малолетний, А.Е. Кудлай, М.Ю. Хоменок

Необходимость расширения приложений беспроводных сенсорных сетей WSN (wireless sensornetwork) и качества предоставляемых услуг явились причиной проведения исследований по разработке этой сети в комбинации с мобильной Ad Hoc сетью MANET (Mobile Ad Hoc Netwoks). MANET как и WNS, используется как в гражданской так и военной областях. В [1] отмечается возможность крупномасштабного развертывания сети WSN-MANET, по технологии smart city, представляющей широкий спектр услуг: мониторинг шума, света, загрязнения окружающей среды, движения транспортных средств, противоугонная защита, контроль по предотвращению обрушения старых зданий, мостов, экстренная медицинская услуга, услуги пожилым людям и др.

Другим значимым примером развертывания сети WSN-MANET в комбинации с летающей Ad Hoc сетью является ЛСС (летающая сенсорная сеть) FANET (Flying Ad Hoc Netwoks), которая включает беспилотные летающие аппараты БПЛА (Unmanned Air Vehicles, UAVs), используемые для удаленного получения изображений, мониторинга стихийных бедствий, видеотрансляции и др. [2]. Сеть FANET имеет более сложные проблемы информационной безопасности (ИБ) по сравнению с MANET. Одними из причин является более высокая мобильность и соответственно более быстрое изменение топологии сети, а также большие расстояния между БПЛА, чем между узлами в MANET.

При проектировании ЛСС стоит задача выбора узла иерархии в качестве шлюза для взаимодействия с группой БПЛА в FANET. При этом важную роль имеет анализ угроз ИБ при получении шлюзом на каждом уровне полных и корректных сенсорных данных. В докладе рассматриваются вопросы обеспечения информационной безопасности ЛСС иерархической структуры от воздействия атак DoS.

Литература

1. Convergence of MANET and WSN in IoT Urban Scenarios / P. Bellavista [et al.]. // IEEE Sensors Journal. – 2013. – Vol. 13, № 10. – P. 3558–3567.

2. Razzaqi, A.A. Antenna array design for multi-UAVs communication in next generation Flying Ad-Hoc Networks (FANETs). High-capacity Optical Networks and Emerging / A.A. Razzaqi, M. Mustaqim, B.A. Khawaja // Enabling Technologies (HONET): 11th Annual. – 2014. – P. 25–28.

О ПРИМЕНЕНИИ СТАТИСТИЧЕСКИХ МЕТОДОВ ДЛЯ ОЦЕНКИ КАЧЕСТВА КРИПТОГРАФИЧЕСКИХ ГЕНЕРАТОРОВ

М.В. Мальцев, В.Ю. Палуха, Ю.С. Харин

Для надежного шифрования необходимы криптографические генераторы – устройства, вырабатывающие последовательности случайных или псевдослучайных чисел. Выходные последовательности криптографического генератора должны быть неотличимы от «чисто случайной» или равномерно распределенной случайной последовательности (РРСП) [1]. Для оценки качества таких выходных последовательностей применяются вероятностно-статистические методы. В частности, критерием надежности генератора может служить энтропия, причем помимо классической энтропии Шеннона перспективным направлением является применение энтропии Тсаллиса и Реньи. Энтропийный анализ используется для статистического тестирования и распознавания криптографических генераторов [2].

Элементы РРСП независимы в совокупности, но псевдослучайные последовательности вырабатываются генераторами по определенным детерминированным алгоритмам и в таких последовательностях присутствуют зависимости, как правило, большой глубины. Для описания таких зависимостей адекватной моделью является цепь Маркова порядка s. К сожалению, использовать ее на практике зачастую невозможно, поскольку число параметров этой модели увеличивается экспоненциально с ростом s. В связи с этим необходимы так называемые малопараметрические марковские модели, число параметров которых зависит от s полиномиально [3]. Авторами данной статьи разработан ряд малопараметрических моделей для анализа зависимостей в выходных последовательностях криптографических генераторов.