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.

Литература

1. Криптология / Ю.С. Харин [и др.]. – Минск: БГУ, 2013. – 512 с.

2. Палуха, В.Ю. Статистические тесты на основе оценок энтропии для проверки гипотез о равномерном распределении случайной последовательности // Вес. Нац. акад. навук Беларуси. Сер. фіз.-мат. навук. – 2017. – №1. – С. 79–88.

3. Мальцев, М.В. Малопараметрические марковские модели в задачах защиты информации / М.В. Мальцев, Ю.С. Харин // Электроника ИНФО. – 2013.– С. 202–207.

СРЕДСТВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОЛОСОВОГО ТРАКТА

М.Г. Матуть, В.А. Вишняков

Контроль телефонных переговоров остается одним из наиболее распространенных видов промышленного шпионажа и действий злоумышленников. Причины – низкий уровень затрат и риск реализации угроз, необязательность захода в контролируемое помещение, разнообразие способов и мест съема информации. В широком смысле можно выделить средства противодействия: физическая защита информации, включающие в себя постановщики заградительных помех, нейтрализаторы, фильтры и средства физического поиска каналов утечки информации; криптографическая защита информации.

Криптофон представляет собой смартфон с установленным специальным программным обеспечением. Современные криптофоны используют, в основном, алгоритмы шифрования AES и Twofish. В сфере IP-телефонии можно рассматривать варианты использования IPsec (Internet Protocol Security) на сетевом уровне, либо протоколы TLS (Transport Layer Security) и SRTP (Secure RTP) на транспортном уровне.

В качестве основы разрабатываемого программного средства был выбран проект с открытым исходным кодом – CSipSimple, который является бесплатным SIP-клиентом, работающим под ОС Android и распространяющимся по лицензии GNU GPL. Выбор CSipSimple обусловлен наличием в нем открытых реализаций протоколов SIP over TLS, SRTP и ZRTP; поддержка различных кодеков (Speex, G.711, GSM-FR, G.729, G.722 и другие) и возможность добавления новых, при помощи плагинов; наличие плагина для осуществления видеозвонков, одновременно может быть активно до 10 аккаунтов.

АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ ЗАЩИТОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СЕТЯХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

А.Р. Мацылевич

Автоматизация управления защитой информации в информационных сетях специального назначения (ИССН) позволит максимально исключить влияние так называемого «человеческого фактора», который является не только фактором, снижающим эффективность системы защиты информации в ИССН, но, в некоторых условиях, становится угрозой безопасности информации высокого потенциала.

Основными вопросами автоматизации управления защитой информации являются:

представление защиты информации как объекта управления (определение входных и выходных переменных, метрик пространства состояний, описание поведения защиты информации в пространстве ее состояний и другие);

постановка целей, определение методов их достижения, а также критериев управления защитой информации адекватных целям, задачам и условиям функционирования ИССН;

разработка порядка применения средств и систем автоматизированного управления защитой информации в ИССН;

разработка методов контроля эффективности и оптимизации управления защитой информации в ИССН с учетом специфики их функционирования.

В настоящее время уже существуют подходы для создания систем управления организационно-техническими процессами, к которым относится защита информации [1]. Одним из подходов в автоматизации управления защитой информации в ИССН является применение научно-методологического аппарата теории автоматического управления.