БЛА. Для преодоления данных ограничений предлагается использовать трехмерный фрактальный хаос при задании параметров группового движения БЛА. В среде MATLAB создана фрактальная хаотическая модель группового движения БЛА на основе клеточного автомата и рекурсивных перестановок. Сущность модели состоит во фрактальном расширении и рекурсивной перестановке элементов исходной хаотической матрицы состояний клеточного автомата небольшого размера для формирования хаотических матриц движения произвольного размера. Модель позволяет сократить вычислительную сложность формирования хаотических матриц движения за счет уменьшения числа операций при фрактальном расширении исходной хаотической матрицы. Произведен анализ телеметрических данных полетов БЛА: высоты, широты и долготы. Установлено, что значения коэффициента Херста, вычисленные с помощью формулы Уиттла, составляют 0.999 для фрактальной хаотической модели и телеметрических данных БЛА. Согласно этим значениям оба процесса являются самоподобными, что позволяет использовать предложенную модель для описания движения группы БЛА. Достоинствами модели являются отсутствие ограничений на число узлов в группе и хаотический характер связей между параметрами движения узлов в группе и между группами.

АНАЛИЗ УЯЗВИМОСТЕЙ МОБИЛЬНЫХ САМООРГАНИЗУЮЩИХСЯ СЕТЕЙ НА СЕТЕВОМ УРОВНЕ

А.А. ПОДЛУЦКИЙ, А.П. БОЛТРУК, К.С.Ш. АЛЬ-САФФАР, В.Ю. ЦВЕТКОВ

Мобильным самоорганизующимся безинфраструктурным сетям (MANET-Mobile AdHoc Networks) в последнее время уделяется большое внимание. Одной из основных их особенностей является то, что каждый узел участвует в маршрутизации трафика. Такой принцип работы сети делает сравнительно легким внедрение вредоносных узлов с целью организации атак на сетевом уровне. Атаки, направленные на протоколы маршрутизации, можно классифицировать как внешние и внутренние, пассивные и активные. Основными идеями при организации атак являются следующие: перенаправление маршрутов и трафика, зацикливание маршрутов, создание перегрузки в узлах сети, переполнение маршрутных таблиц, имитация разделения сети на отдельные подсети, увеличение времени доставки сообщений. Все они в своей основе используют уязвимости протоколов маршрутизации. Защита от внешних атак включает шифрование передаваемой маршрутной информации и обеспечение различных сервисов безопасности. Возможные способы защиты от внутренних атак (при наличии в сети скомпрометированных узлов) предполагают: разделение информации на части и их передача по независимым маршрутам, обнаружение скомпрометированных узлов и исключение их из процесса маршрутизации за счет применения узлами систем обнаружения вторжения. Одной из причин сложности организации безопасности MANET сетей является мобильность их узлов. Однако, мобильность может сыграть и положительную роль при обеспечении безопасности сети. Предлагается использовать паттерны мобильности для формирования статуса доверия к узлу.

СЖАТИЕ ВИДЕОДАННЫХ ВОЗДУШНОГО ЦИКЛИЧЕСКОГО МОНИТОРИНГА НА ОСНОВЕ КАДРОВОЙ КОМПЕНСАЦИИ ДВИЖЕНИЯ ПО ФОТОПЛАНУ

А.А. ЖУРАВЛЕВ, В.Ю. ЦВЕТКОВ, А.С. АЛЬ-АЛЕМ, В.К. КОНОПЕЛЬКО

Видеоанализ в системах безопасности требует высокого качества видеоданных. При осуществлении видеомониторинга с использованием беспилотного летательного аппарата (БЛА) выполнение данного условия проблематично из-за малой пропускной способности радиоканала, требующей значительного сжатия видеоданных. Известные методы сжатия видеоданных, основанные на кадровом кодировании, кодировании кадровой разности и блочной компенсации движения, не эффективны в условиях циклического

Библиотека БГУИР

видеомониторинга на базе БЛА, осуществляемого по постоянному маршруту (патрулирование границ, нефти- и газопроводов, железнодорожных путей, автомагистралей и т.д.). Они не учитывают априорную видеоинформацию о зоне наблюдения, накапливаемую за предыдущие циклы мониторинга, и поэтому не позволяют достичь высоких коэффициентов сжатия без существенного ухудшения качества видеоданных. Предлагается метод сжатия видеоданных воздушного циклического мониторинга на основе кадровой компенсации движения по фотоплану — изображению зоны мониторинга, сформированному вдоль траектории полета БЛА за предыдущие циклы мониторинга. Сущность метода состоит в поиске фрагмента фотоплана, соответствующего опорному кадру, и кодировании координат и коэффициентов трансформации этого фрагмента, а также разности между ним и соответствующим опорным кадром. Предварительное определение границ, ориентации и масштаба области поиска на фотоплане относительно опорного кадра осуществляются по данным GPS и телеметрии. Для повышения эффективности метода необходимо учитывать сезонность, освещенность, ракурс, а также использовать предварительную обработку фотоплана для ускорения поиска соответствующих фрагментов. При выполнении данных требований предлагаемый метод позволяет повысить коэффициент сжатия видеоданных по сравнению с методами MPEG-4 и H.264 за счет использования кадровой разности при кодировании опорных кадров на базе фрагментов фотоплана.

АНАЛИЗ ЭФФЕКТИВНОСТИ ПРОТОКОЛОВ АУТЕНТИФИКАЦИИ В СИСТЕМАХ ВИДЕОКОНФЕРЕНЦСВЯЗИ

А.В. АРТАМОНОВ, Ф.Н.М. АЛЬ-МАШХАДАНИ, А.С. АЛЬ-АЛЕМ, В.Ю. ЦВЕТКОВ

Системы видеоконференцсвязи (ВКС) — важный инструмент в современном ведении бизнеса. Поэтому обеспечение безопасности систем ВКС является актуальной задачей. Анализ безопасности систем программной ВКС Microsoft Lync 2010, Skype и Cisco WebEx показал, что важной составляющей безопасности является аутентификация пользователей в системе ВКС. Для аутентификации пользователей Skype использует протокол TLS, алгоритмы шифрования AES-256, RSA, SHA-1, RC4 и систему цифровой подписи ISO 9796-2. Microsoft Lync 2010 использует протокол Kerberos для аутентификации внутренних пользователей и протоколы TLS-DSK или NTLMv2 для аутентификации внешних пользователей. Шифрование в Microsoft Lync 2010 осуществляется на базе RSA-RC4-128-SHA. WebEx использует протокол SAML 2.0 для аутентификации и технологию шифрования WevEx, основанную на 128-разрядном шифровании по протоколу SSLv3, AES-256. Дополнительно в WebEx предоставляется возможность использования инфраструктуры открытых ключей (PKI) на основе сквозного шифрования. Пароль на подключение к совещаниям WebEx для мобильных пользователей кодируется с использованием 128-разрядного шифра по стандарту DES. Анализ общей защищённости указанных систем ВКС показал, что из-за особенностей архитектуры Skype и постоянной необходимости связи пользователей через Интернет, данная система недостаточно надёжна для использования в корпоративных сетях. Системы ВКС Microsoft Lync и Cisco WebEx предоставляют высокий уровень защиты, поэтому их можно рекомендовать для предоставления безопасных сервисов как внутри локальной, так и в глобальной сетях.

THE VARIANTS OF CHEMICAL MODIFICATION OF POWDERY SCHUNGITE FOR ITS APPLICATION IN SHIELDS OF ELECTROMAGNETIC RADIATION FOR INFORMATION PROTECTION

K.A. KRYSHTOPAVA, TONBARA BARUGU HENRY

Shungit is a natural carbon containing mineral composite the main components of which are globular carbon and silicon oxide in the form of alpha-quartz. Schungite structure which is a carbon

Библиотека БГУИР