Решение задачи сводится к поиску в двух и более полученных изображениях одних и тех же объектов, их сопоставлению, геометрическому преобразованию одного изображения к плоскости другого изображения и конечном слиянии данных изображений для отображения в виде панорамы. Путем исследований для ускорения процесса сопоставления было решено сопоставлять “ближайшие” друг к другу 35% исходных изображений. Контуры основных объектов на изображениях остаются неизменными. Отличия в перекрывающихся частях изображений возникают из-за геометрических искажений при съемке.

После теоретических изысканий было решено воспользоваться алгоритмом выделения границ объектов на основе вычисления порога Отсу для необходимых частей изображений и бинаризацию по данному порогу. После подготовки изображений необходимо произвести их совмещение. Для этого были рассмотрены два различных алгоритма совмещения контуров[1]:

Первый основан на идеях комплексного контурного анализа, а второй на использовании матрицы гомографии. Первый алгоритм позволяет учитывать преобразования изображений: сдвиг вдоль вектора, поворот относительно начала общей системы координат, изменение масштаба. Но он не учитывает проекционные искажения, которые будут возникать при съемке, поэтому он не подходит для совмещения изображений при съемке панорам.

Второй алгоритм - алгоритм совмещения контуров с помощью методов комплексного контурного анализа, позволяет учитывать сдвиг вдоль вектора, изменение масштаба, поворот относительно начала общей для двух изображений декартовой системы координат, что вполне достаточно.

Учесть влияние проекционных искажений можно в алгоритме совмещения контуров с помощью матрицы гомографии. Идея заключается в умножении этой матрицы на вектор, компоненты которого являются координатами i-й точки совмещаемого контура (изображения).

Одним из самых важных достоинств обнаружения объектов в последовательности снимков при съемке панорам и их совмещению с использованием контурного анализа является слабая зависимость точности от искажений яркости при различных условиях съемки, также стоит указать вычислительную простоту алгоритмов контурного анализа, и, следовательно высокую скорость выполнения алгоритма, что свидетельствует о возможности использования в системах реального времени.

Список использованных источников:

1. Логинов А.А., Новиков А.И., Саблина В.А., Щербакова О.В. Исследование возможности применения комплексного контурного анализа в задачах классификации и совмещения контуров // Вестник РГРТУ, №1 (выпуск 43). Рязань, 2013. с.20-25.

АУДИТ БЕЗОПАСНОСТИ ТРАФИКА В СИСТЕМЕ IP-ТЕЛЕФОНИИ

Шабан А.И.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Одинец Д.Н. – к.т.н.,доцент

В данной работе были рассмотрены возможные виды атак при использовании протокола установления связи в системе IP-телефонии. Также рассмотрены методы для повышения безопасности в системе IP-телефонии и предотвращения рассмотренных видов атак.

В IP-телефонии для установления связи между клиентами используется протокол SIP. Структура и синтаксис сообщений похож на те что используется в HTTP, что представляет собой набор текстовых строк, заголовки и тело сообщения разделены пустой строкой.

Протоколы SIP и RTP, используемы для передачи медиа данных, были разработаны без учета необходимости защищать передаваемую информацию, в следствии чего возможны следующие виды атак:

1) Фрод звонков – атакующий проникает в систему IP-телефонии и имеет возможность совершать звонки, украсть пароли и имена пользователей [1];
2) Вирусы – вирус, попавший в сеть IP-телефонии может начать рассылать спам ее абонентам. Т.к. клиенты для IP-телефонии могут быть реализованы в виде программ, то данному виду атаки подвержен не только клиент, но и операционная система, в следствии чего могут быть украдены данные;
3) Нарушение звонков – атакующий рассылает пакеты клиентам звонка, что приводит к ухудшению качества, задержкам и даже прекращению звонка [2];

4) DoS – данная атака нарушает доступность сервиса, также не позволяет авторизованным пользователям использовать сервис. Данная атака может осуществляться за счет отправки большого количества сообщений “Invite” и “Registrer”, что нарушает работу компонентов SIP;
5) Подслушивание – атакующий прослушивает весь трафик в IP-телефонии;
6) Подбор паролей;
7) Man-In-The-Middle – атакующий проникает в звонок между пользователями, и может не только прослушивать, но и изменять сообщения между клиентами.

Для защиты передаваемы данных, может быть использован протокол TLS – протокол защиты транспортного уровня. Данный протокол использует асимметричное шифрования для аутентификации, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений.

Также для защиты данных может быть использован IPsec – набор протоколов для обеспечения защиты данных, передаваемых по протоколу IP, обеспечивающих аутентификацию, проверку целостности и/или шифрование IP-пакетов [3].

При сравнении протоколов TLS и IPsec можно отметить что TLS имеет следующие преимущества:

1) Отсутствие постоянного соединения между сервером и клиентом;
2) Реализуется на уровне представления.

Недостатки:

1) Не может быть использован с протоколом UDP;
2) Требуется отслеживать состояние соединения.

Однако протокол IPsec реализуется на сетевом уровне и позволяет шифровать данные, но при этом сложен в реализации, предъявляет дополнительные требования к оборудованию сети.

Для улучшения защиты может быть использован VPN. В случае невозможности использования VPN, необходимо использовать VLAN. Данные решения создают виртуальную сеть, что позволяет передавать данные в ненадежных сетях [4].

Шифрование это один из ключевых механизмов, не позволяющего атакующему получить ценную информацию из перехваченных сообщений.

На данный момент аутентификация происходит в два этапа, что не является надежным методом. CHAP – протокол аутентификации с косвенным согласованием. Является алгоритмом проверки подлинности и предусматривает передачу не самого пароля пользователя, а косвенных сведений о нём. Аутентификация узла выполняется путём трехэтапной процедуры согласования.

Преимущества CHAP:

1) Значение идентификатора и переменного значения открытого ключа возрастают, что предотвращает атаки повторного воспроизведения;
2) Метод проверки подлинности основан на том, что аутентификатору и узлу известен секрет, который никогда не посылается по каналу.

Анализ трафика может быть осуществлен при помощи DIP, что позволяет анализировать содержимое передаваемых пакетов и блокировать вирусы.

Для передачи медиа данных необходимо использовать SRTP, который предназначен для шифрования, установления подлинности сообщения, целостности данных.

Для шифрования данных, SRTP использует алгоритм AES, который может использоваться в двух режимах:

1) Сегментированный целочисленный счётчик — режим, который осуществляет произвольный доступ к любым блокам, что является существенным для трафика RTP, передающегося в публичных сетях с непредсказуемым уровнем надежности и возможной потерей пакетов. AES, работающий в этом режиме, является алгоритмом шифрования по умолчанию, с длиной шифровального ключа по умолчанию в 128 бит и ключом сессии длиной в 112 бит;
2) f8-режим — вариант режима способа обратной связи, расширенного, чтобы быть доступным с изменённой функцией инициализации. Значения по умолчанию для шифровального ключа и ключа сессии — то же, что и в AES в режиме.

Рассмотрев приведенные методы защиты, нужно отметить, что для обеспечения безопасного соединения, необходимо использовать TLS, т.к. данный протокол реализуется на транспортном уровне и не требует поддержки данного протокола на промежуточных устройствах, в отличаи IP-Sec.

Так как TLS не обеспечивает защиту сообщений в случае их перехвата, то необходимо воспользоваться шифрованием данных. В данном случае лучшим выбором будет использование VPN который позволяет шифровать данные, так как в этом случае нет необходимости реализовывать шифрование на клиентах и повышает совместимость, отсутствует риск ошибок в реализации шифрования, VPN может быть обновлен для использования более современных методов шифрования без необходимости обновления кода клиента.

Так же необходимо использовать аутентификацию CHAP. Для передачи медиа информации должен использоваться протокол SRTP.

Список использованных источников:
1. http://www.centurylinkbrightideas.com/how-to-address-voip-security-challenges
2. https://habr.com/en/company/pt/blog/212839/
3. https://www.researchgate.net/publication/235601569_SIP_Server_Security_with_TLS_Relative_Performance_Evaluation
4. https://searchunifiedcommunications.techtarget.com/feature/SIP-network-security-measures

ОСНОВНЫЕ ЭТАПЫ 3D РАСПОЗНАВАНИЯ ЛИЦ

Шакун Р.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Лукашевич М.М. – к.т.н.,доцент

Трехмерная информация о поверхности лица человека является мощной биометрической модальностью, которая может повысить точность идентификации и проверки точности систем распознавания лиц в сложных ситуациях. При наличии вариантов освещения, выражения и позы традиционные алгоритмы распознавания лиц на основе двумерных изображений обычно сталкиваются с проблемами. С доступностью трехмерной (3D) информации о форме лица, которая по своей природе не чувствительна к освещению и создает изменения, эти сложности могут быть эффективно устранены

Система 3D распознавания лиц обычно состоит из следующих этапов: получение 3D образцов лица, предобработка образцов, извлечение признаков, запись признаков в базу, поиск соответствий между признаками.

Рабочий процесс может быть разбит на две фазы(обучения и тестирования) и пять этапов. Первым этапом обучения является сбор данных. Получение трехмерных образцов лица включает в себя специальное аппаратное оборудование, которое можно отнести к категории активных систем сбора данных и пассивных систем сбора данных в соответствии с используемыми технологиями. Активные системы сбора данных излучают невидимый свет, например, инфракрасные лазерные лучи, чтобы осветить лицо человека. Затем системы измеряют отражение, чтобы определить особенности формы целевой грани. Пассивные системы содержат несколько камер, которые расположены отдельно друг от друга. Система сопоставляет точки, наблюдаемые с другой камеры, и рассчитывает точное трехмерное местоположение совпадающей точки. Набор совпавших точек формирует трехмерное лицо.

Полученные трехмерные данные лица не могут быть непосредственно использованы в качестве входных данных алгоритмов извлечения признаков, поскольку данные содержат отвлекающие элементы, такие как волосы, уши, шея, очки и ювелирные изделия. Такие особенности, как волосы, очки и украшения, могут время от времени меняться, а особенности ушей и шеи не могут быть достоверно идентифицированы в разных позах головы, поэтому, дабы не вводить в заблуждение алгоритмы распознавания, они должны быть удалены до извлечения признаков.

Следующим этапом предварительной обработки является определение положения и ориентации человеческого лица. Геометрические преобразования используются для «поворота» человеческого лица непосредственно к оси камеры. Затем предварительная обработка использует помощь от четко определенных частей лица, таких как нос, чтобы изолировать область человеческого лица от областей отвлекающих элементов. Эта операция называется сегментацией.

Предварительно обработанные образцы лицевых данных часто интерпретируются в трех форматах модели: глубинное изображение, облако точек и сетка.

Затем для обработки данных применяются алгоритмы извлечения признаков, чтобы найти те, которые можно использовать для распознавания лиц. Самый простой способ выделения признаков состоит в том, чтобы рассматривать все лицо как единый вектор признаков, который называется глобальным подходом [1]. При таком подходе все лицо сохраняется в базе данных. На этапе сопоставления признаков лицо цели сравнивается с лицами в базе данных с использованием статистических классификационных функций. В противоположность глобальному подходу, компонентный подход фокусируется на локальных характеристиках лица, таких как нос и глаза. Он использует операторы графа для извлечения части носа и глаз и сохранения этих локальных особенностей в базе данных. Когда целевая грань вводится для распознавания, компонентный подход сначала извлекает соответствующие детали из целевых граней, а затем ищет соответствующий набор деталей из базы данных объектов. Существуют гибридные подходы, которые объединяют функции, используемые глобальными и локальными подходами. При более высоких