

Боб производит измерение переданного состояния, в одном из двух возможных базисов А или В, выбранном независимо от Алисы. Если базис, выбранный Бобом для измерения, совпадает с базисом, выбранным Алисой для передачи, биты данных у Алисы и Боба будут идентичны. В противном случае они совпадут с вероятностью 50%. Алиса и Боб повторяют эту процедуру N раз, в результате чего каждый из них будет обладать строкой бит длиной N.

На второй стадии общение Алисы и Боба происходит по открытому каналу, который, однако, должен соответствовать следующему условию: Ева не может изменять передаваемые сообщения. Алиса и Боб сообщают друг другу использованные ими при передаче значения базисов и договариваются исключать из своих данных те биты, для которых базисы передачи и детектирования не совпадали. Результирующая строка бит называется сырым ключом.

Ева в свою очередь может перехватывать носители информации, посланные Алисой, измерять их состояния и пересылать далее Бобу. Эта стратегия называется «перехват/регенерация». Поскольку Ева вынуждена выбирать базисы для детектирования случайно и независимо от Боба и Алисы, то приблизительно в 50% случаев базисы Евы и Боба не совпадут. А так как измерения Боба случайны и примерно на 50% совпадают с данными Алисы, то вероятность правильного результата будет 75%. Это означает, что Алиса и Боб должны сравнить публично некоторое случайно выбранное подмножество своих данных на наличие ошибок.

Существует, однако, еще один способ подслушивания, известный как «расщепление луча». Особенность его состоит в том, что Алиса и Боб не могут определить наличие такого рода подслушивания в канале. Известно, что при используемом повсеместно способе получения одиночных фотонов, а именно, ослаблении лазерного излучения до средней интенсивности $I \leq 1$ фотона на импульс, определенная доля выходного излучения будет содержать более одного фотона в импульсе. Таким образом, поставив на пути фотонов обыкновенный делитель, Ева может получить некоторую информацию о ключе, не внося ошибок в передачу.

Все это справедливо лишь для идеального квантового канала, в реальном же канале всегда присутствуют шумы, и некоторое несоответствие в данных Алисы и Боба будет всегда, даже в отсутствие подслушивания. Так как Алиса и Боб не могут различить ошибки, имеющие причиной подслушивание, и ошибки, вызванные естественными шумами канала, то им приходится предполагать, что все ошибки передачи вызваны присутствием Евы. При этом стадия обмена по открытому каналу усложняется.

Рассмотренные атаки объединяет то, что для осуществления подслушивания измерительная аппаратура Евы каким-либо образом взаимодействует с передаваемыми квантовыми состояниями. Однако существует возможность подслушивать эти схемы либо, не имея дела с квантовыми состояниями вообще, либо, детектируя их однозначно при помощи некоторой дополнительной информации, почерпнутой во время передачи. Такой тип атак получил название

«тройанский конь». При этом одиночный сканирующий импульс, посланный Евой, вызовет множество отраженных сигналов с различными амплитудами, задержками и фазами, и все они в разной степени пригодны для успешного выполнения данной атаки.

Существуют различные методы защиты данных, передаваемых Алисой. Один из них заключается в постановке аттенюатора на выходе передающего интерферометра. При этом источник одиночных фотонов для передатчика делается путем ослабления лазерных импульсов до средней интенсивности порядка 0,1 фотона на импульс. Для Евы присутствие аттенюатора на выходе приемника будет означать значительное увеличение требуемой мощности лазера.

Еще одним методом защиты является измерение входящей оптической мощности в передающем и приемном интерферометрах для предупреждения легальных пользователей о несанкционированном проникновении в канал. Т.к. для Евы имеется достаточно широкий выбор длин волн, на которых может осуществляться сканирование, то целесообразно использовать узкополосные чувствительные детекторы вместе с полосовыми фильтрами на выходе передатчика и входе приемника, вместо широкополосных измерителей оптической мощности.

РАЗРАБОТКА ПРОГРАММНО-РЕАЛИЗУЕМОГО УЗЛА ДОСТУПА ПАКЕТНОЙ СЕТИ

Юрасов С.В.

*Нижегородский Государственный
Технический Университет,
Н.Новгород*

Безусловно, пропускная способность сетей в современном информационном мире невероятно важна. Однако, на сегодняшний день возможности сетевых магистралей таковы, что оптические технологии и современные методы мультиплексирования обещают не только удовлетворить самые высокие требования, но и создать некоторую избыточность полосы пропускания. Тем не менее, ряд приложений, таких, как видео, мультимедиа, передача голоса по IP-сетям, требует не просто «толстых» каналов, а и соответствующего качества обслуживания – QoS (Quality of Service). Иными словами, в сложившейся ситуации на первый план выходит скорость обработки пакетов. И здесь вся нагрузка ложится на активные элементы сетевой инфраструктуры – маршрутизаторы, коммутаторы, узлы доступа и другие устройства, участвующие в формировании трафика в пакетных сетях.

Ни для кого не секрет, что для конечного пользователя сеть – это не компьютеры, кабели и концентраторы, и даже не информационные потоки, для него сеть – это, прежде всего, тот набор сетевых служб и услуг, с помощью которых он получает возможность просмотреть список имеющихся в сети компьютеров, прочитать удаленный файл, распечатать документ на «чужом» принтере или послать почтовое сообщение. Именно совокупность предоставляемых возможностей – насколько широк их выбор, насколько они удобны, надежны и безопасны – определяет для

• ользователя облик той или иной сети. Таким образом, главным требованием, предъявляемым к сети, является выполнение сетью ее основной функции – обеспечение пользователям потенциальной возможности доступа ко всем услугам и службам сети. Вот тут то и выходят на сцену такие сетевые устройства как узлы доступа – *access point*.

Access Point (узел доступа, в дальнейшем AP) – это интерфейс, предоставляющий конечным пользо-

вателям доступ к ядру сети. Узел доступа обеспечивает доступ конечного пользователя к разнообразным услугам сети. Под *предоставлением доступа* понимается трансляция запросов EU (End User – конечных пользователей) к сетевым службам (например, почтовая служба, служба обмена файлами, служба поддержки телеконференций и т.д.) и передачи ответов этих служб.

Основные функции AP:
1) Связь с узлом более высокого уровня;
2) Передача трафика между различными компонентами узла (маршрутизация);
3) Конвертер протоколов;
4) Поддержка и контроль качества обслуживания (QoS);

Дополнительные функции AP:
1) Поддержка Firewall;
2) Поддержка VPN;
3) Поддержка VoIP;
4) Поддержка протокола SNMP для осуществления мониторинга и управления.
5) и др.

Точки доступа, поддерживающие всю вышеперечисленную функциональность, безусловно, уже существуют и широко используются, однако они абсолютно статичны, а наиболее важным расширением функциональности AP на текущий момент является возможность автоматического поиска и загрузки программного обеспечения для поддержки запрашиваемого конечным пользователем сервиса. Отсюда возникает вопрос, какими техническими средствами можно реализовать сетевое устройство, которое могло бы быстро «обучаться» в условиях бурного роста сетевых сервисов. И вообще возможно ли?

Вплоть до начала 90-х годов традиционные сетевые устройства базировались на архитектуре, подобной персональному компьютеру. Существенным недостатком таких устройств, приобретшим особую остроту сегодня, является их весьма ограниченная возможность поддерживать высокие скорости передачи и расширять набор функций. Когда же таким устройствам приходится заниматься фильтрацией трафика, осуществлять маршрутизацию на основе правил (политик) или собирать статистику о своей работе, то их производительность значительно снижается, следовательно, возникает необходимость в увеличении рабочих мощностей.

Ситуация начала существенно меняться, когда получили распространение заказные микросхемы (Application-Specific Integrated Circuit - ASIC), процессоры цифровой обработки сигналов (Digital Signal Processor - DSP) и RISC-процессоры. Появление ASIC привело к некоторому сдвигу в парадигме у производителей аппаратного обеспечения. Они увидели, что вместо того, чтобы повышать частоту процессоров для получения требуемой производительности, они могут достичь большего эффекта с помощью специализированных чипов со встроенными инструкциями. Такое решение позволяет управлять трафиком аппаратными средствами, что повышает пропускную способность устройств. Это не только открыло еще один сегмент рынка для производителей микросхем, но и позволило им предлагать запрограммированные и готовые к использованию чипы, на базе которых могли быть быстро разработаны новые аппаратные решения. Применение ASIC породило новое поколение очень быстрых коммутаторов и маршрутизаторов.

Однако в полном соответствии с законами диалектики такой подход нес в себе и отрицание, в конце концов, заставившее от него отказаться. Дело в том, что логика, "намертво" встроенная в чипы, с трудом поддавалась модификации, что не позволяло оперативно расширять функциональность и улучшать производительность, и тем более добавлять новую функциональность «на лету». Ошибки в дизайне существенно увеличивали сроки выхода продукта на рынок, а реализация многих дополнительных функций, таких, как QoS, идентификация потока данных на высоких уровнях модели OSI или управление доступом, все еще выполнялась на программном уровне, сводя на нет преимущества ASIC-базированной архитектуры.

На текущий момент ИТ-индустрия предлагает сетевые процессоры, провозглашая их панацеей, позволяющей избежать эффекта «бутылочного горлышка» и обеспечить необходимый уровень всему разнообразию сетевого трафика, а так же делает возможным создание «обучающихся» сетевых устройств, так необходимых в условиях огромного роста числа сетевых служб и сервисов. Именно по этому пути пошла корпорация Intel, создавая линейку своих сетевых процессоров IXP. И рассмотрение именно этой проблемы – созданию обучающихся сетевых устройств, т.е. загрузке функционального кода для изменения возможностей узла доступа или, иначе говоря, созданию **программно-реализованного узла доступа** (Software Defined Network Element), является целью данной работы.

Для достижения поставленной цели в ходе работы были решены следующие задачи:

- проведен технический анализ IX архитектуры;
- проведена разработка UML-модели программно-реализуемого узла доступа.
- проведена демонстрация возможностей IXP процессоров для построения программно - реализованных узлов доступа. В качестве демонстрационного проекта было разработано программное обеспечение для осуществления мониторинга и управления точкой доступа на базе платформы IXP1200EB, а так же для дистанционной загрузки функционального кода;

- произведено полное, комплексное тестирование разработанной системы.

Сетевое направление корпорация Intel развивает весьма активно и, безусловно, IX архитектура будет являться единой универсальной базой для создания разработчиками сетевых устройств различного назначения - от маршрутизаторов для локальных сетей (LAN) уровня предприятия до коммутаторов территориально распределенных сетей (WAN) и многофункциональных маршрутизаторов. Очевидно, что создание узла доступа пакетной сети на базе процессора с IX архитектурой и возможностью дистанционной за-

грузки функционального кода – а как следствие возможностью менять функциональность сетевого узла «на лету» дают нам новый тип сетевого оборудования, так называемый SDNE – Software Defined Network Element (программно-реализованный сетевой элемент), во многом отличающийся от современных узлов доступа. Данный тип сетевого оборудования в силу своей относительной дешевизны, мобильности и расширяемости имеет огромное будущее в области IT-индустрии.

Диагностика, терапия, профилактика социально значимых заболеваний человека

ИЗУЧЕНИЕ ВЛИЯНИЯ ПРОБУКОЛА НА НЕКОТОРЫЕ ПОКАЗАТЕЛИ ПЕРЕКИСНОГО ОКИСЛЕНИЯ ЛИПИДОВ КРЫС С W-256 НА ФОНЕ ЭКСПЕРИМЕНТАЛЬНОЙ МИОКАРДИОДИСТРОФИИ, ПОЛУЧАВШИХ РУБОМИЦИН

Соломанина О.О., Микуляк Н.И., Кинзирский А.С.
Пензенский государственный университет,
Пенза

Среди лекарственных средств, регулирующих процессы перекисного окисления липидов нами выбран пробукол, обладающий выраженной антиоксидантной активностью. Снятие показателей перекисного окисления липидов проводили в день забоя животных на 25 день эксперимента. Все экспериментальные животные были распределены на IV группы, по 8 особей в каждой группе: I – интактная группа; II – группа – крысы с перевитой W-256 на фоне экспериментальной миокардиодистрофии, индуцированной доксорубицином (W-256+CH); III – группа - крысы с перевитой W-256 на фоне экспериментальной миокардиодистрофии, индуцированной доксорубицином и получавшие рубомицин в дозе 4 мг/кг в/б, 4-хкратно, через 48 часов, начиная с 8 суток после перевивки опухоли (W-256 +CH+P); IV – группа - крысы с перевитой W-256 на фоне экспериментальной миокардиодистрофии, индуцированной доксорубицином и получавшие рубомицин в дозе 4 мг/кг в/б, 4-хкратно, через 48 часов, начиная с 8 суток после перевивки опухоли и пробукол внутривенно, в дозе 50 мг/кг, начиная с 6-х суток после имплантации опухолевых клеток в течение 16 дней (W-256+CH+ПБ+P). В качестве дополнительного контроля в исследовании была включена группа интактных животных.

В данных опытах исследовали влияние рубомицина и пробукла на уровень МДА, Fe-МДА и каталазы в сыворотке крови и миокарде экспериментальных животных. Как показали результаты исследований во II группе (W-256+CH) животных, которые получали доксорубин наблюдалось достоверное увеличение уровня МДА в сыворотке крови на 64% ($p<0,05$), а содержание Fe-МДА остается на исходном уровне по отношению к интактным животным. Дополнительная нагрузка другим антибиотиком – рубомицином, крысы III группы W-256 +CH+P увеличивала содержание

МДА в сыворотке крови на 86,1% ($p<0,05$), а содержание Fe-МДА на 66,7% ($p<0,001$). Пробукол в используемой дозе эффективно снижает содержание МДА в сыворотке крови по сравнению с контрольной группой на 43,7% ($p<0,05$). Активность каталазы во всех опытных группах достоверно не изменялась, по сравнению с интактной группой.

Во II группе животных (W-256+CH), которым вводили доксорубин, отмечается достоверный рост уровня МДА в миокарде на 92,4% по отношению к интактным, при этом увеличивается содержание и Fe-МДА на 61,9% ($p<0,01$). Значения вышеперечисленных показателей более значимо увеличены у животных III группы (W-256 +CH+P), которые получали рубомицин. Эффективно снижает уровень МДА в миокарде пробукол: на 40% по отношению ко II группе (W-256+CH). Достоверно снижается и концентрация Fe-МДА – на 49,9%, по сравнению со II группой и в то же время на 18,9% от уровня интактного контроля ($p<0,01$).

Нами показано, что в условиях совместного применения рубомицина и пробукла терапевтическая эффективность первого полностью сохраняется. Пробукол восстанавливает уровень МДА, Fe-МДА в сыворотке крови и миокарде крыс с W-256 и экспериментальной миокардиодистрофии при совместном введении с рубомицином.

ОЦЕНКА МИКРОЦИРКУЛЯТОРНОГО РУСЛА БРЫЖЕЙКИ ТОНКОЙ КИШКИ КРЫС (БТК) МЕТОДОМ ВИТАЛЬНОЙ МИКРОСКОПИИ ПРИ КОРРЕКЦИИ ТЕРМИЧЕСКОГО ОЖОГОВОГО ШОКА ПЕРФТОРАНОМ

Мейланова Р.Д., Магомедов М.А.
Дагестанская Государственная
Медицинская Академия, ЦНИЛ,
Махачкала

Исследовались изменения микроциркуляции при экспериментальном термическом ожоговом шоке и через 6 и 24 часа после коррекции его коррекцией перфтораном. Работа проведена на 30 белых беспородных крыс весом 180-200г.