Скрытное подсоединие к оптоволокну: методы и предосторожности

las68 — Read time: 11 minutes

Скрытное подсоединие к оптоволокну: методы и предосторожности

13 мин

110K

Статьи по прослушиванию оптоволокна достаточно редки в силу определенной специфики такого рода коммуникаций. По мере удешевления оборудования и стоимости организации каналов связи на основе оптоволокна, они давно применяются в коммерческой практике. Специалистам ИТ, отвечающим за вопросы безопасности коммуникаций, стоит знать об основных источниках угроз и методах противодействия. Данная статья представляет собой перевод научной работы, опубликованной в материалах конференции HONET (High Capacity Optical Networks and Enabling Technologies) в 2012 году. В сети удалось найти полнотекстовый авторский препринт, датированный осенью 2011 года, который, хотя и содержит некоторые ошибки (авторы не являются оригинальными носителями английского языка), тем не менее достаточно хорошо описывает существующие проблемы.

Скрытное подсоединие к оптоволокну: методы и предосторожности

М. Зафар Икбал, Хабиб Фатхалла, Незих Белхадж

M.Z IQBAL, H FATHALLAH, N BELHADJ. 2011. Optical Fiber Tapping: Methods and Precautions. High Capacity Optical Networks and Enabling Technologies (HONET).

Аннотация

Связь с использованием оптоволокна далеко не так безопасна, как это обычно принято считать. Существует ряд известных методов, используемых для извлечения или вставки информации в оптический канал и позволяющих избежать обнаружения подключения. Ранее сообщалось о нескольких инцидентах, в которых успешное подключение было сложно обнаружить. В данной работе рассматривается ряд известных методов подключения к оптоволокну, приводится отчет о симуляции оптических характеристик волокна, к которому подсоединение выполнено методом сгиба, а также доказательство концепции в виде

физического эксперимента. Также представлены схемы различных сценариев, где злоумышленник, обладающий необходимыми ресурсами и использующий существующие технологии, может скомпрометировать безопасность оптического канала связи. Обсуждаются способы предотвращения подключения к оптоволокну, либо минимизации последствий утечки информации, передаваемой по каналу связи.

Данная статья основана на работе, поддерживаемой Королевскими ВВС Королевства Саудовская Аравия.

М. Зафар Икбал работает в Исследовательском Институте Продвинутых Технологий Принца Султана (ziqbal@ksu.edu.sa)
Хабиб Фатхалла – доцент (помощник профессора) Университета Короля Сауда(hfathallah@ksu.edi.sa)
Незих Белхадж – постдок-исследователь Универитета Лаваля (nbelhadj@gel.ulaval.ca)

I. ВВЕДЕНИЕ

В противоположность общему представлению, оптоволокно, по существу, не имеет защиты от сторонних подключений и прослушивания. В настоящее время по оптическим каналам связи передается огромное количество критической и чувствительной информации, и есть риск того, что она может попасть в руки определенных лиц, имеющих необходимые ресурсы и оборудование.

Подключение к оптоволокну (fiber tapping) – процесс, при котором безопасность оптического канала компрометируется вставкой или извлечением световой информации. Подключение к оптоволокну может быть интрузивным либо неинтрузивным. Первый метод требует перерезания волокна и подсоединения его к промежуточному устройству для съема информации, в то время как при использовании второго метода, подключение выполняется без нарушения потока данных и перерыва сервиса. Неинтрузивным технологиям и будет посвящена данная статья.

В настоящее время сообщается лишь о нескольких зафиксированных случаях подключения к оптоволокну. Это связано с большими сложностями в обнаружении места подключения, в то время как собственно подключение выполняется достаточно просто. Вот список основных инцидентов:

- 2000, В аэропорту Франкфурта, Германия обнаружено подключение к трем главным линиям компании Deutsche Telekom [1].
- 2003, на оптической сети компании Verizone обнаружено подслушивающее устройство [1].
- 2005, подводная лодка ВМФ США USS Jimmy Carter модернизирована специальным образом для установки несанкционированных подсоединений к подводным кабелям [2],[3] (*Отдельный пост на хабре — Подводная лодка USS Jimmy Carter, её специальные задачи и подводные оптические кабели*).

В следующих разделах мы представим краткий обзор способов неавторизованного подключения [4]. Затем мы представим численное представление потери сигнала при сгибании волокна, сопровождаемое отчетом о физической демонстрации прототипа устройства для подключения к оптоволокну, разработанного в нашей лаборатории. Здесь же мы объясним устройство прототипа, используемое при этом оборудование и программное обеспечение. Также мы обсудим возможные сценарии подключения в реальных условиях и обговорим, какие ресурсы нужны для достижения этих целей. В итоге мы предложим несколько методик по защите оптических каналов против подсоединений.

II. МЕТОДЫ ПОДСОЕДИНЕНИЯ К ОПТОВОЛОКНУ

A.Сгибание волокна

При данном методе подключения, кабель разбирается до волокна. Данный способ основан на принципе распространения света через волокно посредством полного внутреннего отражения. Для достижения данного способа угол падения света на переход между собственно ядром волокна и его оболочкой должен быть больше, чем критический угол полного внутреннего отражения.

В противном случае, часть света будет излучаться через оболочку ядра. Значение критического угла является функцией показателей отражения ядра и его оболочки и представлено следующим выражением:

$\theta_c = \cos^{-1}(\mu_{cladding} / \mu_{core})$, причем $\mu_{cladding} < \mu_{core}$;

Здесь θ_c – критический угол, $\mu_{cladding}$ — показатель преломления оболочки, μ_{core} — показатель преломления ядра

При сгибании волокна, оно искривляется таким образом, чтобы угол отражения стал меньше чем критический, и свет начал проникать через оболочку

Очевидно, что могут быть два типа сгибов:

1) Микросгиб

Приложение внешнего усилия приводит к острому, но при этом микроскопическому искривлению поверхности, приводящему к осевым смещениям на несколько микрон и пространственному смещению длины волны на несколько миллиметров (рис.1). Через дефект проникает свет, и он может использоваться для съема информации.

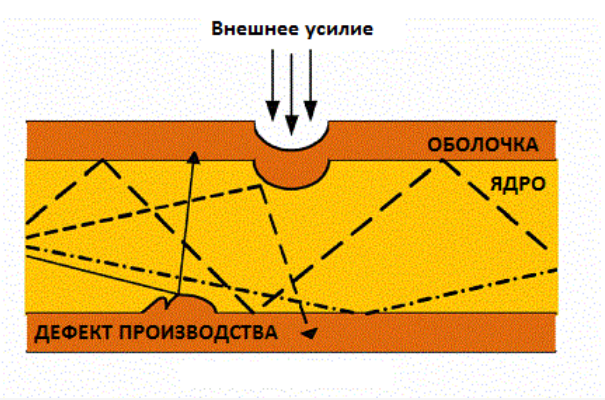

Рисунок 1.Микроизгиб

2) Макросгиб

Для каждого типа волокна существует минимально допустимый радиус изгиба. Это свойство также может использоваться для съема информации. Если волокно сгибается при меньшем радиусе, то возможен пропуск света (рис.2), достаточный для съема информации. Обычно минимальный радиус изгиба одномодового волокна составляет 6.5-7.5 см, за исключением волокна специального типа. Многомодовое волокно может быть изогнуто до 3.8 см.

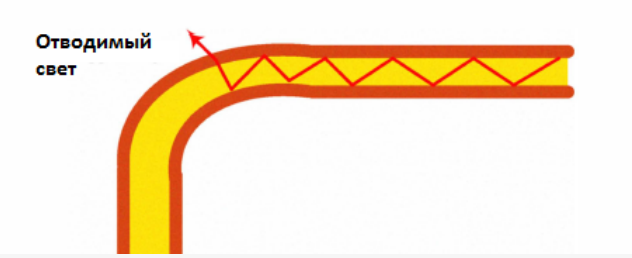

Рисунок 2. Макроизгиб

B. Оптическое расщепление

Оптоволокно вставляется в сплиттер, который отводит часть оптического сигнала. Этот метод является интрузивным, поскольку требует разрезания волокна, что вызовет срабатывание тревоги. Однако, необнаруженное подключение такого типа может работать годами.

C. Использование неоднородных волн (Evanescent Coupling)

Данный способ используется для перехвата сигнала от волокна-источника в волокно-приемник посредством аккуратной полировки оболочек до поверхности ядра и затем их совмещения. Это позволяет некоторой части сигнала проникать во второе волокно. Данный способ трудновыполним в полевых условиях.

D. V-образный вырез (V Groove Cut)

V-образный вырез – это специальная выемка в оболочке волокна близкая к ядру, сделанная таким образом, что угол между светом, распространяющимся в волокне и проекцией V-выреза больше, чем критический. Это вызывает полное внутреннее отражение, при котором

часть света будет уходить из основного волокна через оболочку и V-образный вырез.

E. Рассеяние

На ядре волокна создается решетка Брэгга, с ее помощью достигается отражение части сигнала с волокна. Это достигается наложением и интерференцией УФ лучей, создаваемых лазером с УФ возбуждением.

III. МОДЕЛИРОВАНИЕ

A. Методология

Для точной оценки потерь при сгибании оптоволокна типа SMF-28 используется полновекторный частотный решатель Максвелла, основанный на методе конечных элементов высокого порядка и допускающий адаптацию граничных условий — растягивающегося идеально согласованного слоя. Получены векторные расчеты констант распространения и электрических полей мод в изогнутых волноводах. Потери при сгибе рассчитываются на основе мнимой части константы распространения фундаментальной моды. Общие потери получены сложением потерь ортогональной и базовой моды. Результаты, полученные данным способом достаточно точны и были проверены в [5].

B. Данные для моделирования.

Для волокна SMF-28, радиус ядра и показатель преломления представляют собой соответственно.
r_c = 4.15 μm и n_c=1.4493
В оболочке, они соответственно равны:
r_{cl} = 62.25 μm and n_{cl}=1.444.
Коэффициент преломления воздуха равен 1.

C. Расчет потери мощности.

Радиус изгиба ρ взят по оси x, мода поляризуется вдоль оси y, а распространение идет по оси z, как показано на рисунке 3.

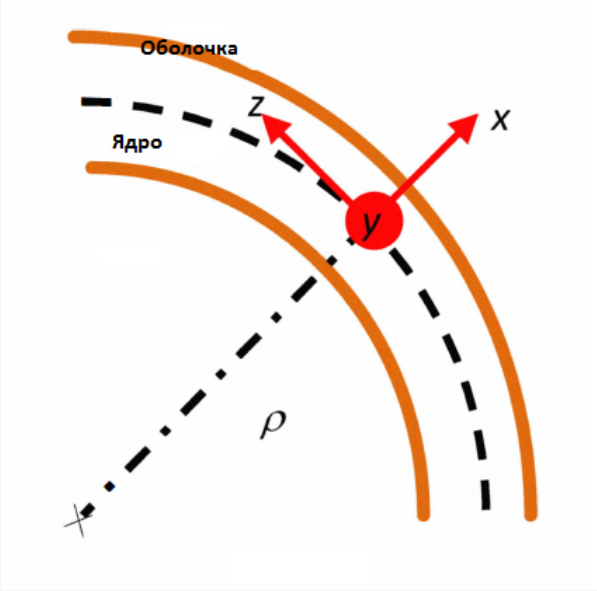

Рисунок 3

Рисунок 4 представляет собой выраженную в числах потерю на сгибе как функцию радиуса изгиба волокна метровой длины. Наблюдается логарифмическая зависимость потерь относительно радиуса изгиба. Для небольших радиусов изгиба (ρ < 10 mm), потери превышают 40 dB/м. При обычных радиусах изгиба (ρ > 15 mm) потери составляют меньше чем 1 dB/м

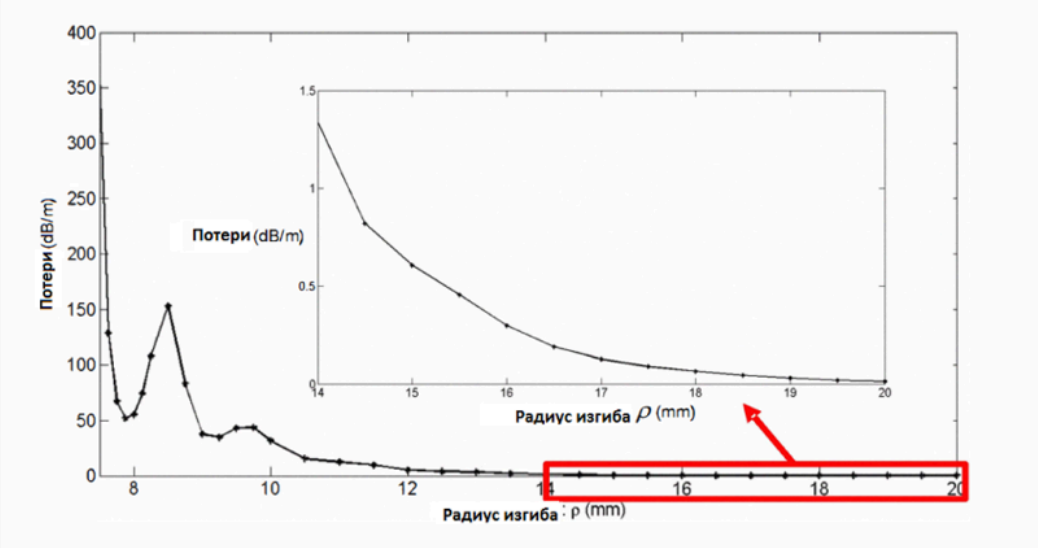

Рисунок 4. Численная оценка потери на изгибе, как функции от радиуса изгиба

IV. ЭКСПЕРИМЕНТ ПО ПОДКЛЮЧЕНИЮ К ОПТОВОЛОКНУ

A. Последовательность действий при подсоединении к оптоволокну.

Полностью операция прослушивания может быть реализована с помощью следующих шагов:

1. Получение оптического сигнала с волокна
2. Детектирование сигнала.
3. Обнаружение механизма передачи (декодирование протокола)
4. Программная обработка обнаружения фреймов/пакетов и извлечение из них необходимых данных.

Эксперимент включал в себя передачу цифрового видеосигнала через оптический Ethernet с одного компьютера на другой. Подсоединяемое волокно было разделано до оболочки и помещено в оптический каплер (coupler), где волокно сгибается, вызывая излучение некоторого количества света, нарушающего принцип полного внутреннего отражения. Это устройство направляет захваченный свет в однонаправленный конвертер Ethernet. В дальнейшем, фреймы Ethernet обрабатываются и из них реконструируется видеопоток на третьем ПК. Для передачи потока и воспроизведения использовался VLC плеер. Анализатор протоколов WireShark использовался для захвата пакетов, а ПО Chaosreader использовалось для реконструкции видео из захваченных пакетов.

B. Процедура

Программное и аппаратное обеспечение соединено как на рисунке 5. Разделанное волокно проходит от источника видео до приемника, через зажим каплера. В зажиме отводится часть света и попадает в однонаправленный медиаконвертер, считывающий Ethernet-фреймы, которые затем передаются в третий PC, на котором стоит WireShark. Анализатор протокола конвертирует фреймы Ethernet и извлекает такую информацию как MAC –адреса источника и приемника. Также он обрабатывает содержимое фреймов и достает из него IP-пакеты. Информация, полученная из пакетов, включает в себя IP-адреса, сообщения сигнальных протоколов и биты служебной загрузки.

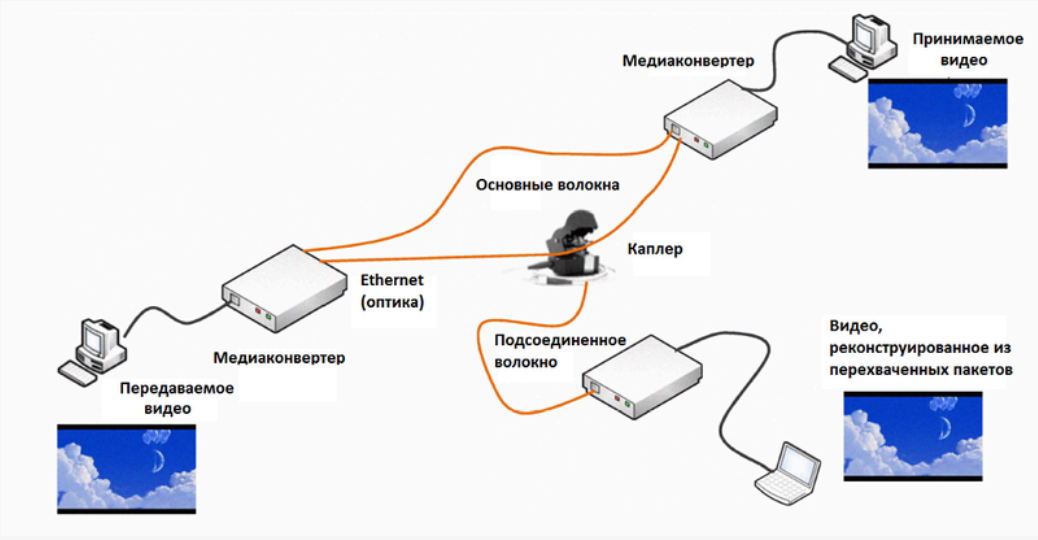

Рисунок 5.Экспериментальная схема для подсоединения к волокну методом изгиба

Пакеты собранные таким способом сохраняются в формате файла pcap (packet capture). Затем файл обрабатывается ПО Chaosreader, который реконструирует оригинальные файлы и создает индекс реконструированных файлов. Для обнаружения нашего захваченного видео, мы смотрим в каталоге и ищем *.DAT файлы большого размера. Затем этот файл открывается в плеере VLC и показывает перехваченную часть видеопотока.

C.Возможные действия при прослушке

Помимо проигрывания видео, экспериментальная система, описанная здесь, может быть использована для выполнения ряда задач по перехвату

информации, такой например как сведения для атаки по IP-адресам, кражи паролей, прослушивания VoIP-переговоров, реконструкции сообщений электронной почты с помощью бесплатного, коммерческого или самодельного ПО.

V. ДАЛЬНЕЙШИЕ СЦЕНАРИИ ПОДСОЕДИНЕНИЯ.

Эксперимент, описанный здесь, выполнялся с использованием Ethernet компонентов, по причине их наибольшей доступности. Однако, некоторые сценарии, возможные в реальной жизни, вполне могут выглядеть так:

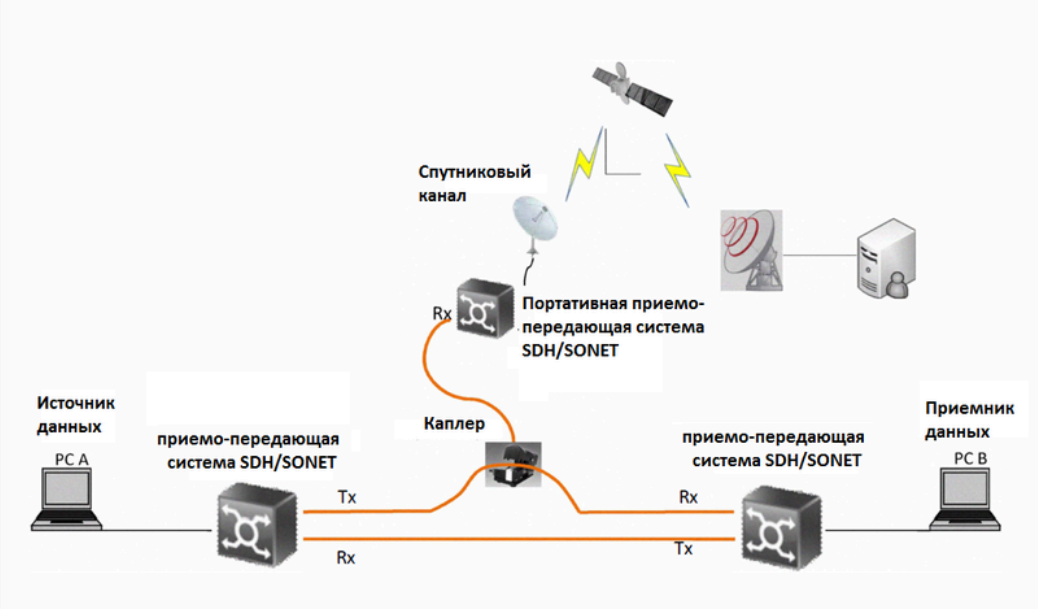

Рисунок 6 Сценарий подсоединения с удаленной обработкой.

A.Подсоединение к сети передачи данных

.

Ценная информация может быть получена из сетей передачи данных таких как SDH и SONET — двух основных стандартов передачи данных по оптоволокну через магистральные каналы связи и метросети.

Информацию из высокоскоростных сетей достаточно сложно сохранять и обрабатывать, но на рынке доступны высокотехнологичные анализаторы SDH-протоколов, которые могут быть использованы для получения низкоуровневых исходных сигналов[6].Частично это упрощает возможные сложности, связанные со скоростью передачи данных. Такие устройства могут быть впоследствии доработаны для получения различных типов трафика, проходящего через сеть. Например, можно извлекать ethernet поток, который сопоставлен некоторому потоку контейнера VC4.

Подсоединение с удалённой обработкой

Существует две важных стимула заниматься удаленной обработкой:

- При подключении к дальним высокоскоростным (несколькоГбит/сек) каналам связи, роль хранилища становится крайне важной. Захваченные пакеты заполняют диск крайне быстро.

- Привлечение сетевых экспертов для работы в полевых условиях может оказаться весьма затратным. Более удобно организовать им работу в удаленном центре обработки где присутствует любое необходимое оборудование, сложно выносимое в поле.

При использовании воображения, можно легко достроить все необходимые сценарии по работе с удаленными данными. Например:

1) Использование беспроводного интернета. При использовании Wi-Fi, прослушивающий компьютер может находиться в другой комнате или фургоне, за пределами здания, где установлено подключение. Эксперт может работать в относительной безопасности с возможностью доступа ко всем ресурсам.
2) Использование микрочастотного или спутникового канала. Наша экспериментальная схема была модифицирована и Ethernet трафик перенаправлялся на направленный спутниковый канал (рис.6).
3) Вставка сигнала.При помощи метода рассеяния, описанного ранее, теоретически возможно создать устройство, которое имеет возможность передавать сигнал внутрь волокна посредством видоизмененной технологии оптического каплинга (coupling)
Можно разработать технологии для постановки помех на волокно без разрыва в связи или даже внедрение зловредной информации.

VI. ЗАЩИТА ОТ ПОДКЛЮЧЕНИЙ.

Есть три основных категории методов предотвращающих или снижающих до минимума влияние посторонних подключений:

A. Наблюдение за кабелем и мониторинг.

1. Мониторинг сигналов вблизи волокна.

Производство оптоволокна с дополнительными волокнами, по которым передается специальный сигнал мониторинга. Использование такого метода увеличит стоимость кабеля, но любая попытка согнуть кабель вызывает потерю сигнала мониторинга, и вызывает срабатывание сигнала тревоги [7].

2) Электрические проводники

Другой метод состоит в интегрировании электрических проводников в кабель, и если оболочка кабеля нарушена, то изменяется емкость между электрическими проводниками и это может использоваться для срабатывания тревоги.

3) Мониторинг мощности мод.

Этот метод применим к мультимодовому волокну, в котором затухание – это функция от моды, в которой распространяется свет. Подсоединение влияет на определенные моды, но при этом затрагивает и другие моды.

Это приводит к перераспределению энергии от проводящих мод к непроводящим, что меняет соотношение энергии в ядре волокна и его оболочке. Изменение энергии в модах может быть обнаружено на принимающей стороне соответствующим измерением, что будет являться информацией для принятия решения – есть подключение к кабелю или нет [8].

4) Измерение оптически значимой мощности

В волокне может осуществляться мониторинг уровня оптически значимой мощности. В том случае, если она отличается от установленного значения, срабатывает сигнал тревоги. Однако это требует соответствующей кодировки сигнала, так чтобы в волокне присутствовал постоянный уровень сигнала, не зависящий от наличия передаваемой информации [8].

5) Оптические рефлектометры

Поскольку подсоединение к волокну забирает часть оптического сигнала, для обнаружения подключений могут использоваться оптические рефлектометры. С их помощью можно установить расстояние по трассе, на котором обнаруживается падение уровня сигнала (рис.7) [8]

Рисунок 7. Поиск подключения на оптической трассе с помощью оптического рефлектометра

6) Методы с использованием пилотного тона:

Пилотные тоны проходят по волокну также как и коммуникационные данные. Они используются для обнаружения перерывов в передаче. Пилотные тоны могут использоваться для обнаружения атак, связанных с постановкой помех, но если несущие волновые частоты пилотных тонов не затрагиваются, то данный метод не является эффективным при обнаружении такого рода атак. О наличии подключения можно судить только по существенной деградации уровня сигнала пилотного тона [8]

В. Сильногнущееся волокно.

Эти виды волокна, обычно называемые волокном с низкими потерями и сильным радиусом изгиба, защищают сеть передачи данных, ограничивая высокие потери, возникающие при прокалывании волокна или его сгибании. Кроме того, для светового потока становятся менее

повреждающими такие факторы как вытягивание, перекручивание и другие физические манипуляции с волокном. Существуют также другие типы волокна основанные на иных технологиях производства [9].

C. Шифрование

Хотя шифрование никак не препятствует подсоединению к волокну, она делает украденную информацию малополезной для злоумышленников. Шифрование обычно классифицируется по уровням 2 и 3.

1) Шифрование третьего уровня

Пример шифрования третьего уровня – протокол IPSec. Он реализуется на стороне пользователя, так что это вызывает определенные задержки в обработке. Протокол поднимается вначале сессии и общая реализация может быть весьма сложной если в работу вовлечено большое количество сетевых элементов. Рассмотрим, например, разработку мультимедийных подсистем. При первоначальной разработке, связь между различными узлами и элементами является незащищенной. Существенно позже IPSec был встроен в оригинальный дизайн, так как технологии нижнего уровня не предлагали никакого шифрования вообще.

2) Шифрование второго уровня.

Шифрование второго уровня освобождает элементы третьего уровня от любого бремени шифрования информации. Один из возможных источников шифрования второго уровня – это оптический CDMA, который считается относительно безопасным [10-12]. Данное допущение, в основном, базируется на методах расшифровки методом грубой силы и упускает из виду более продвинутые способы. Вероятность успешного перехвата данных является функцией нескольких параметров, включая отношение сигнал/шум, и дробление (fraction) доступной системной емкости. В [12] указывается что увеличение сложности кода может увеличить отношение сигнал/шум, требуемое для злоумышленника чтобы «сломать» кодирование всего лишь на несколько dB, в то время как обработка менее чем 100 бит со стороны злоумышленника может уменьшить отношение сигнал/шум на 12 dB. Перепрыгивание по длинам волн и распределение сигнала во времени в частности, и использование O-CDMA в общем, обеспечивают достаточный уровень секретности, но он высоко зависит от системного дизайна и параметров реализации.

БЛАГОДАРНОСТИ

Авторы благодарят Исследовательский Институт Продвинутых Технологий Принца Султана за предоставление его ресурсов и выполнение экспериментальной части работы.

VII. ЗАКЛЮЧЕНИЕ

Подсоединение к оптоволокну является весьма осязаемой угрозой интересам национальной безопасности, финансовым организациям а также персональной приватности и свободам. После подключения,

получаемая информация может быть использована многими способами в зависимости от мотивации злоумышленника и его технических возможностей. В данной работе мы предоставили концепцию как в виде симуляции, так и в виде физического эксперимента, используя подключение посредством ‘подключения методом сгиба’ и также продемонстрировали возможность существования разных сценариев, выполнимых при помощи доступных технологий. Помимо получения информации с оптоволокна, существует ряд методик, позволяющих вставлять информацию в неё, как в случае с разделением на неоднородных волнах и достигнуть постановки помех или вброса неверной информации. Явная легкость прослушивания оптоволокна требует определенных предосторожностей, что также описано в этой статье.

ССЫЛКИ

1. Sandra Kay Miller, «Hacking at the Speed of Light », Security Solutions Magazine, April 2006
2. Davis, USN, RADM John P.«USS Jimmy Carter (SSN-23): Expanding Future SSN Missions». Undersea Waifare, Fall 1999 Vol.2, No. I
3. Optical Illusion by: Sandra Kay Miller Information security Issue: Nov 2006.
4. Optical Network Security: Technical Analysis of Fiber Tapping Mechanisms and Methods for detection and Prevention, Keith Shaneman & Dr. Stuart Gray, IEEE Military Communications Conference 2004.
5. R. Jedidi and R. Pierre, High-Order Finite-Element Methods for the Computation of Bending Loss in Optical Waveguides, lLT, Vol. 25, No. 9, pp. 2618-30, SEP 2007.
6. FTB-8140 Transport Blazer — 40143 Gigabit SONETISDH Test Module, EXFO
7. «Optical Fiber Design for Secure Tap Proof transmission», US Patent No. 6801700 B2, Oct. 5,2004.
8. All Optical Networks (A ON), National Communication System, NCS TIB 00-7, August 2000
9. DrakaElite, BendBright-Elite Fiber for Patch Cord, Draka Communications, July, 2010
10. W. Ford, «Computer Communications Security», Upper Saddle River, NJ: Prentice-Hall, 1994.
11. D. R. Stinson, «Cryptography», Boca Raton, FL: CRC, 1995.
12. N. Ferguson and 8. Schneier, «Practical Cryptography», Indianapolis, IN: Wiley, 2003.