УДК 621.391.63

АТАКИ НА ПАССИВНЫЕ ОПТИЧЕСКИЕ СЕТИ СО СТОРОНЫ АБОНЕНТСКОГО ОКОНЧАНИЯ

Н.Н. СЕРГЕЕВ, В.Н. УРЯДОВ, С.С. ШИШПОРЁНОК

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 22 июня 2018

Аннотация. Проведен анализ принципов построения пассивных оптических сетей. Рассмотрены варианты атак на PON-сеть, а также атаки со стороны абонентского окончания. Проведена оценка возможности таких атак. Предлагается метод защиты от атак путем применения схемы WDM-PON.

Ключевые слова: пассивная оптическая сеть, защита информации, несанкционированный доступ, сетевая атака, угроза.

Abstract. The analysis of construction principles of passive optical networks was carried out. Options for attacks on PON-network and attacks from the subscriber were discussed. The possibility of such attacks was evaluated. Method of protection from attacks by use of scheme of WDM-PON was proposed.

Keywords: passive optical network, information security, unauthorized access, network attack, threat.

Doklady BGUIR. 2018, Vol. 114, No. 4, pp. 5-10
Attacks on passive optical networks from the subscriber end
N.N. Sergeev, V.N. Uryadov, S.S. Sheshporenok

Введение

Технология пассивных оптических сетей PON – молодая, постоянно развивающаяся технология, и на сегодняшний день имеется небольшая часть работ, затрагивающих вопросы надежности и живучести сетей связи, построенных на основе данной технологии. Под живучестью понимается свойство сети сохранять свою работоспособность под воздействием вредных факторов, способных вызвать повреждения отдельных ее участков.

Переход от электронных технологий к фотонным несет не только существенные преимущества, но и новые проблемы для информационной безопасности. Появляются новые возможные угрозы. Сегодня можно с легкостью вывести из строя весь сегмент сети, используя всего одну абонентскую розетку, или, к примеру, можно получить доступ к информации, передающейся по пассивной оптической сети, а зафиксировать эту утечку практически невозможно. Поэтому проблема повышения конфиденциальности информации в сетях, построенных на основе технологии PON, стремительно возрастает [1]. Целью работы является исследование возможности несанкционированного доступа к информации, передаваемой в пассивных оптических сетях, при атаках с соседних абонентских розеток.

Архитектура оптических сетей доступа

Под пассивными оптическими сетями (PON) понимают сети, в которых передача оптического сигнала между центральным узлом и множеством абонентских узлов осуществляется пассивными статическими компонентами, без усиления, регенерации/ретрансляции и т. п. активными компонентами. Суть технологии в том, что между приемопередающим модулем центрального узла OLT (Optical line terminal) и удаленными абонентскими узлами ONT (Optical network terminal) создается полностью пассивная оптическая сеть, имеющая топологию дерева. В промежуточных узлах дерева размещаются пассивные оптические разветвители (сплиттеры) –

компактные устройства, не требующие питания. Один приемопередающий модуль OLT позволяет передавать информацию множеству абонентских устройств ONT. Число ONT, подключенных к одному OLT, может быть настолько большим, насколько позволяет бюджет мощности и максимальная скорость приемопередающей аппаратуры. Принцип действия и основные элементы подробно рассмотрены в п. 5 ТКП 300.

Разновидности угроз в сетях PON

Для понимания содержания угрозы информации используется понятие сценария угрозы. Под сценарием угрозы будем понимать последовательность действий нарушителя (злоумышленника), направленных на получение доступа к конфиденциальной информации, и их техническое обеспечение. Используя электрические, акустические, электромагнитные и другие сигналы, злоумышленник по параметрам этих сигналов может получить доступ к передаваемой, хранимой или обрабатываемой информации. Под объектом информатизации будем понимать автоматизированные системы передачи различного уровня и назначения. В пассивной сети конфиденциальную информацию содержит внутренний и внешний трафик. Рассмотрим варианты атак в сетях PON, представленных на рис. 1.

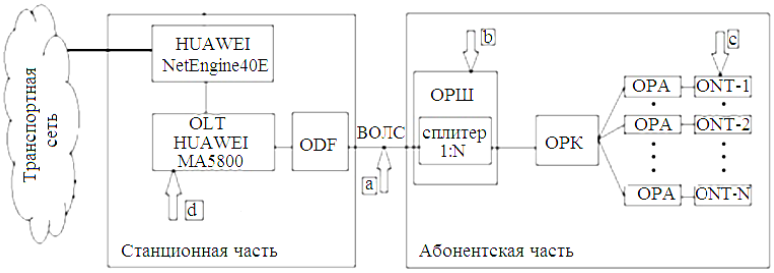

Рис. 1. Варианты атак в сетях PON: *a* – снятие информации с волоконно-оптической линии; *b* – атака на оптические разветвители; *c* – атака на оконечном оборудовании; *d* – атака на стыке сетей

Система безопасности PON сетей должна уметь противостоять такого рода угрозам [2]. Рассмотрим варианты атак на пассивную оптическую сеть [3]:

1. *Перехват информации с волоконно-оптической линии*. В местах изгиба и в местах сварных соединений оптического кабеля световые лучи могут выходить за его пределы. При повреждении изоляции оптического кабеля и подключении специальных средств для регистрации излучения с поверхности волокна злоумышленник получает доступ к данным, передающимся через оптический кабель. Зафиксировать утечку информации на концах кабеля практически невозможно. Угрозами информации в линиях связи являются: прослушивание каналов связи; повреждение кабельной линии связи; уничтожение или искажение информации, проходящей по линиям связи; внедрение ложных сообщений в общий поток, а также сетевых вирусов.

2. *Атака на оптические разветвители (сплиттеры)*. Сплиттеры – это пассивные оптические «делители», которые устанавливаются в местах разветвления оптического кабеля в линии PON; могут быть установлены в общедоступных местах. Для их защиты применяются оптические распределительные шкафы в антивандальном исполнении, имеющие комбинированные замки.

3. *Атака на стыке сетей*. Центральный сервисный модуль линейного терминала OLT находится на стыке между локальной и глобальной сетями. Он содержит коммутатор/маршрутизатор 2, 3 уровня и системный контроллер, позволяющий оператору подключиться к системе управления: локально – через порт RS-232 (RJ-45) или дистанционно – через внешнюю сеть.

Угрозами на сети PON в оборудовании стыка сетей могут быть: ошибочные действия обслуживающего персонала; внесения изменений в программное обеспечение оборудования обслуживающим персоналом; несанкционированное копирование информации с носителей оконечного оборудования обслуживающим персоналом или пользователями.

4. *Атака на оконечное оборудование.* Основной особенностью всех PON сетей является то, что нисходящий поток достигает все оптические сетевые терминалы (ONT), подключенные к сети. Нисходящий поток (downstream) от центрального узла к абонентам идет на длине волны 1490 нм и 1550 нм для видео. Восходящие потоки (upstream) от абонентов идут на длине волны 1310 нм с использованием протокола множественного доступа с временным разделением TDMA.

Следовательно, к каждому терминалу ONT приходят пакеты, адресованные терминалам ONT в пределах данного сплитера. ONT, используя множественный доступ с временным разделением, выбирает из потока адресованный ему пакет.

Очевидно, что злоумышленник после некоторых манипуляций с перепрограммированием ONT или подключением ПК с установленным специальным программным обеспечением к ONT может добиться того, что будет получать информацию, адресованную другим пользователям, всего лишь подобрав необходимый интервал. Это можно сделать с каждой оптической розетки (ОРА).

Используя всё ту же самую оптическую розетку, а доступ к ней получить весьма легко, злоумышленник так же может вывести из строя весь сегмент сети путем примитивного засвета лазером в линию. Это произойдёт в том случае, когда мощность излучаемого в линию сигнала превысит допустимую мощность фотодиода OLT.

Снятие информации нисходящего потока достаточно просто реализуемо, поскольку обычный приемник обеспечивает прием сигнала любого приемника, если использовать другой временной интервал. Более сложно в реализации снятие информации контролируемого абонента с другой абонентской розетки, поскольку используется отраженный сигнал от ответвителя или разъемного соединения. При использовании отраженного сигнала необходимо учесть, что в пассивной оптической сети существуют возвратные потери в неоднородностях.

Рассмотрим модель участка сети длиной L (рис. 2), состоящего из n строительных длин l ($L = nl$) и одного разветвителя $1\times m$ (m – количество абонентов). Затухание разветвителя α_p, в случае передачи информации от ONT-1 к ONT-2, будет весомым, а затухание сигнала на стыках α_c и затухание сигнала в разъемном соединении α_{pc} будут настолько малы, что их в данном случае можно не учитывать.

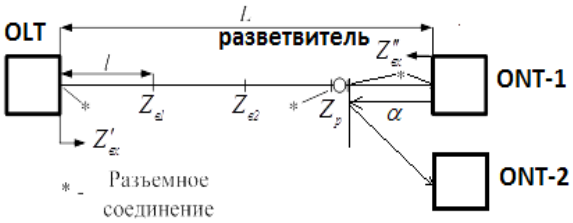

Рис. 2. Поток информации в пассивной оптической сети

Возвратные потери определяют долю оптической мощности, которая возвращается обратно к источнику оптического сигнала. Возвратные или обратные потери определяются в отраженном свете по выражению

$$\alpha_B = -10Lg\frac{P_{îòð}}{P_{âõ}} = -10Lg\frac{(n-n_c)^2}{n^2+n_c^2}, [\text{dB}], \qquad (1)$$

где $P_{вх}$ и $P_{отр}$ – мощности падающего и отраженного излучения соответственно. Основным фактором, определяющим возвратные потери, являются френелевские отражения.

С этой позиции разветвитель характеризуется затуханием на ближнем конце, равным 50 дБ [4]. В соответствии с рекомендацией G984 уровни сигнала любого абонентского передатчика определены. Рассмотрим параметры волоконно-оптического интерфейса в восходящем направлении для класса сети А на различных скоростях (таблица).

Зависимость возбуждаемой мощности от скорости передачи в восходящем направлении

Скорость передачи в восходящем направлении	155,52 Мбит/с	622,08 Мбит/с	1244,16 Мбит/с
Минимум (MIN) средней возбуждаемой мощности	–6 дБм	–6 дБм	–3 дБм
Максимум (MAX) средней возбуждаемой мощности	0 дБм	–1 дБм	+2 дБм

На графике (рис. 3) приведены уровни сигналов, отраженных при использовании разветвителя.

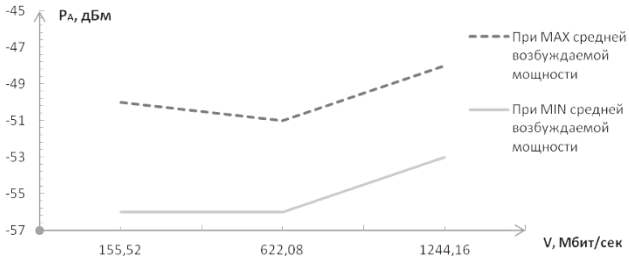

Рис. 3. Уровни отраженных сигналов на выходе ответвителя на разных скоростях

Для определения возможности принятия оптического сигнала на абонентской розетке, с которого снимается информация, рассчитаем чувствительность оптического приемника которую можно получить в квантовом пределе.

Квантовый предел детектирования определяется шумами, связанными с сигналами. Падающий на фотодиод стационарный световой поток генерирует пары носителей заряда как независимые случайные события. Такой процесс преобразования фотонов называется пуассоновским. Если за отрезок времени на фотодиод упадет оптическая энергия, равная в среднем ε_R, то следует ожидать, что будет создано N пар носителей заряда, следовательно [4]

$$E_R = \frac{N \cdot E_{\hat{o}}}{\eta} = \frac{h \cdot c \cdot N}{\lambda \cdot \eta}. \qquad (2)$$

Рассчитаем минимальную среднюю мощность на входе фотоприемника на разных скоростях для каждого N:

$$\overline{\Phi_R} = \frac{1}{2} \cdot E_R \cdot B. \qquad (3)$$

Эти величины характеризуют квантовый предел детектируемости. Чувствительность в дБм на различных скоростях для каждого N определим выражением

$$P = 10 \lg \frac{\hat{O}_R}{10^{-3}}, \text{ äÁì}. \qquad (4)$$

Результы расчета чувствительности приемника на различных скоростях и для разной вероятности ошибки приведены на рис. 4.

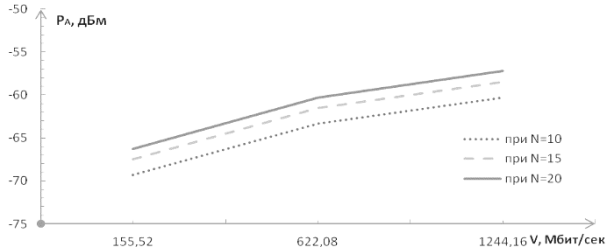

Рис. 4. Зависимость чувствительности фотоприемника от скорости передачи

Чем больше скорость передачи, тем больше требуемая минимальная средняя мощность фотоприемника, а с увеличением минимальной средней мощности фотоприемника его чувствительность уменьшается. Таким образом, для того чтобы воспользоваться отраженным сигналом и снять информацию абонента с другой соседней оптической розетки, достаточно, чтобы величина отраженного сигнала была теоретически в рамках квантового предела детектируемости.

Использование WDM технологии в пассивных оптических сетях для защиты от атак с абонентского окончания

WDM-PON – будущее технологии PON, использующая волновую сетку DWDM для размещения большого количества параллельных высокоскоростных каналов поверх одной структуры PON. WDM-PON предлагает альтернативу схеме передачи, основанной на разделении во времени, как в GPON, схемой, где каждый ONT передает и принимает данные на определенной длине волны. Типичная архитектура WDM-PON будет заменять пассивные сплиттеры на волновые селективные фильтры, которые часто реализованы как решетка на основе массива волноводов (Arrayed Waveguide Grating –AWG).

AWG (решетка волновода) – это пассивный оптический прибор с особенной характеристикой, которая позволяет использовать AWG одновременно в роли мультиплексора и демультиплексора. Решетка AWG направляет каждую отдельную длину волны к одному выходному порту, отделяя несколько длин волн одновременно.

Вносимые потери в AWG около 4–5 дБ (независимо от количества каналов), и это гораздо меньше, чем у оптических кроссов. На рынке недавно появились холодные маршрутизаторы AWG, которые разработаны с термической компенсацией, и у которых применяются материалы с температурным коэффициентом [5].

Достоинства WDM-PON:

– абоненту предоставляется выделенная полоса для приёма и передачи (нет распределения на конкурентной основе);

– сигналы абонентов физически изолированы;

– эффективно используется волокно (до 64 абонентов на волокно);

– возможно значительное увеличение дальности связи (используя AWG с низкими потерями, вместо неэффективных с точки зрения потерь сплиттеров при стандартном для GPON бюджете в 28 дБ, можно подключать абонентов на расстоянии порядка 80 км).

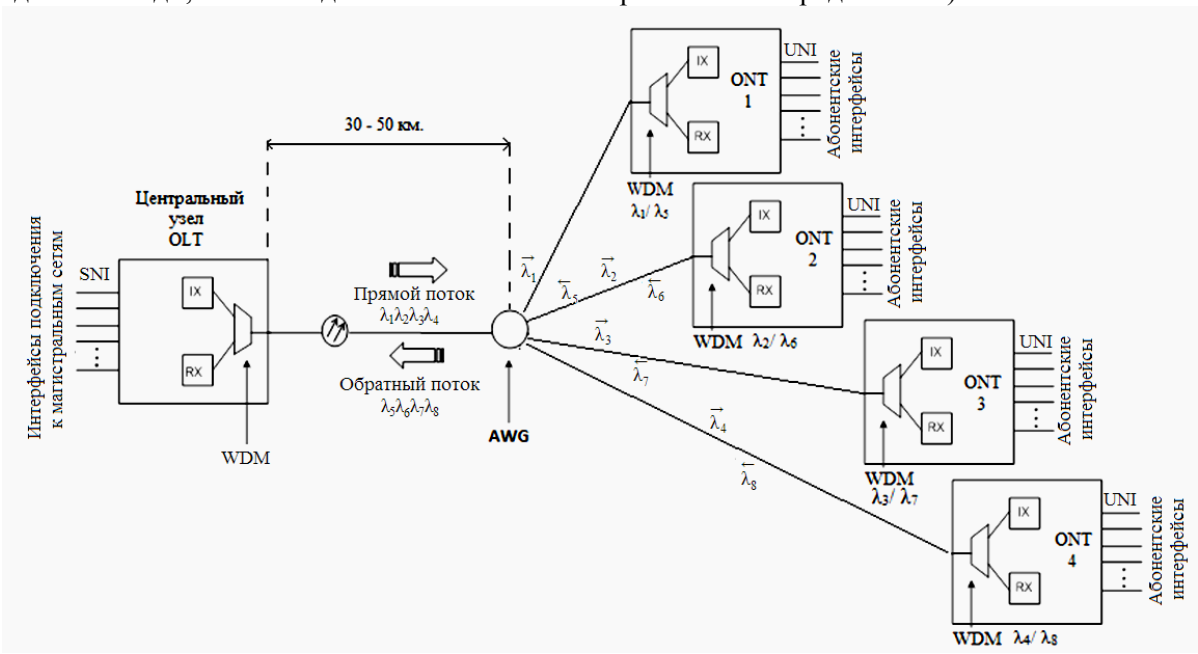

Рис. 5. PON с разделением абонентов по длине волны

Основной недостаток WDM-PON – высокая стоимость, так как требуются узкополосные передатчики, излучающие на заданной длине волны. Это особенно критично для абонентских устройств ONT, так как их стоимость напрямую влияет на стоимость абонентской линии. С одной стороны, проблема частично решается за счет унификации и уменьшения типов аппаратных компонент в оконечных устройствах (например, использование настраиваемых на заданную волну лазеров), с другой – не без оснований можно надеяться, что через несколько лет к моменту выхода стандарта стоимость оптических компонент для WDM-PON будет значительно ниже нынешнего уровня.

Заключение

Показано, что в стандартной сети PON возможен скрытый доступ к передаваемой информации при атаке с любой соседней оптической розетки. Выделяя тайм-слот прямого и отраженного сигнала в оптическом сплиттере – обратного канала, достаточно, чтобы величина этого сигнала была теоретически в рамках квантового предела детектируемости.

Используя WDM-PON, можно избежать данной атаки на пассивные оптические сети со стороны абонентского окончания, так как каждому абоненту приходит сигнал на его длинах волн, при этом существенно увеличиваются еще и возможности сети: предоставление абоненту требуемой полосы пропускания, дальность связи, а также количество абонентов.

Список литературы

1. Птицын Г.А. Живучесть динамических сетей телекоммуникаций. М.: МТУСИ. 2008. 48 с.
2. Gutierrez D., Cho J., Kozovsky L.G. TDM-PON Security Issues: Upstream Encryption is Needed // Optical Fiber Communication and the National Fiber Optic Engineers Conference. California, USA, 25–29 March 2007.
3. Булавкин И.А. Вопросы информационной безопасности сетей PON // Технологии и средства связи. 2006. IW2. С. 104–108.
4. Рекомендация МСЭ-Т G.983.1. Широкополосные оптические сети доступа на базе пассивных оптических сетей.
5. Урядов В.Н., Алишев Я.В. Перспективные информационные технологии в волоконно-оптических сетях телекоммуникаций. Минск, 2003. 191 с.

References

1. Pticyn G.A. Zhivuchest' dinamicheskih setej telekommunikacij. M.: MTUSI. 2008. 48 s. (in Russ.)
2. Gutierrez D., Cho J., Kozovsky L.G. TDM-PON Security Issues: Upstream Encryption is Needed // Optical Fiber Communication and the National Fiber Optic Engineers Conference. California, USA, 25–29 March 2007. (in Russ.)
3. Bulavkin I.A. Voprosy informacionnoj bezopasnosti setej PON // Tehnologii i sredstva svjazi. 2006. IW2. S. 104–108. (in Russ.)
4. Rekomendacija MSJe-T G.983.1. Shirokopolosnye opticheskie seti dostupa na baze passivnyh opticheskih setej. (in Russ.)
5. Urjadov V.N., Alishev Ja.V. Perspektivnye informacionnye tehnologii v volokonno-opticheskih setjah telekommunikacij. Minsk, 2003. 191 s. (in Russ.)

Сведения об авторах

Сергеев Н.Н., аспирант кафедры инфокоммуникационных технологий Белорусского государственного университета информатики и радиоэлектроники.

Урядов В.Н., к.т.н., доцент, доцент кафедры инфокоммуникационных технологий Белорусского государственного университета информатики и радиоэлектроники.

Шишпорёнок С.С. магистрант кафедры инфокоммуникационных технологий Белорусского государственного университета информатики и радиоэлектроники.

Information about the authors

Sergeev N.N., PG student of department of infocommunication technologies of Belarusian state university of informatics and radioelectronics.

Uryadov V.N., PhD, associate professor, associate professor of department of infocommunication technologies of Belarusian state university of informatics and radioelectronics.

Sheshporenok S.S. master student of department of infocommunication technologies of Belarusian state university of informatics and radioelectronics.

Адрес для корреспонденции

220013, Республика Беларусь,
г. Минск, ул. П. Бровки, 6
Белорусский государственный университет
информатики и радиоэлектроники
тел. +375-17-293-23-30;
e-mail: uryadov@bsuir.by
Урядов Владимир Николаевич

Address for correspondence

220013, Republic of Belarus,
Minsk, P. Brovki st., 6
Belarusian state university
of informatics and radioelectronics
tel. +375-17-293-23-30;
e-mail: uryadov@bsuir.by
Uryadov Vladimir Nikolayvich