БЕЗОПАСНОСТЬ ПЕРЕДОВЫХ ОПТИЧЕСКИХ КОММУНИКАЦИОННЫХ СЕТЕЙ СВЯЗИ

Курбонов Саидкомил Саибахромович
Магистр в Ташкентском университете информационных технологий мн. Мухаммада ал-Хоразмий

АННОТАЦИЯ

Возросший спрос на услуги передачи данных в течение последних нескольких лет вызвал соразмерное увеличение пропускной способности каналов, большинство из которых содержат конфиденциальную информацию, личные данные, банковские счета, номера кредитных карт, документы, являющиеся собственностью, и многое другое. В результате существует два типа защиты связи: защита пользовательских данных и защита физической сети. В данной статье мы рассматриваем безопасность передовых оптических сетей связи, волоконно-оптических и открытой оптической связи (FSO – free-space optics). Здесь описывается квантовая криптография и квантовое распределение ключей.

Ключевые слова. *Оптические сети связи, волоконно-оптические сети связи, конфиденциальность, защита, квантовая криптография.*

ABSTRACT

The increased demand for data services over the past few years has caused a commensurate increase in bandwidth, most of which contain sensitive information, personal data, bank accounts, credit card numbers, proprietary documents and more. As a result, there are two types of communications security: user data protection and physical network protection. In this article, we look at the security of advanced optical communications networks, fiber optics and open optical communications (FSO - free-space optics). It describes quantum cryptography and quantum key distribution.

Keywords. *Optical communication networks, fiber-optic communication networks, confidentiality, protection, quantum cryptography.*

ВВЕДЕНИЕ

Быстрое развитие и внедрение плотного мультиплексирования с разделением по длине волны (DWDM - Dense Wavelength Division Multiplexing) в современной оптической сети связи обеспечивает беспрецедентную пропускную способность в одном волокне.

Решение проблемы узкого места доступа с помощью оптоволокна до помещений (FTTP - Fiber to the home) и передовых беспроводных методов (3G, WiMax и т.д.) вызывает спрос со стороны конечного пользователя на более высокую скорость передачи данных, а также на новые услуги передачи данных, большинство из которых содержат конфиденциальную информацию, персональные данные, банковские счета, номера кредитных карт, конфиденциальные документы и многое другое. Это предоставляет злоумышленникам собирать информацию, имитировать источник, изменять данные, переполнять сеть, что уже вызвало международную озабоченность частного сектора и правительства [1].

ОБСУЖДЕНИЕ И РЕЗУЛЬТАТЫ

В целом, существует три типа безопасности в коммуникациях: пользовательские данные, физические сети, управление сетью и обеспечение безопасности.

– Безопасность пользовательских данных решается с помощью алгоритмов шифрования, неуязвимость которых зависит не столько от сложности алгоритма, сколько от предположения, что его слишком сложно взломать с помощью последовательного алгоритма; то есть, он использует неспособность злоумышленника использовать быстрый суперкомпьютер. Это предположение уже не годится, поскольку несколько "неуязвимых" шифров уже были взломаны. Поэтому в настоящее время ведутся серьезные исследования по разработке неуязвимости шифров, основанных на квантово-механических принципах, известных как квантовая криптография, которая использует принцип отсутствия клонирования, поляризацию и запутанность фотонов.

– Физическая безопасность сети, особенно в современных волоконно-оптических сетях, является довольно новой темой. Причина аналогична той, что и с безопасностью пользовательских данных: она использует безыскусность и неспособность злоумышленника перехватить оптоволоконную среду.

– Управление сетью и предоставление услуг относится к сетевым атакам для отключения, управления и перепрофилирования узлов. Если доступ может быть получен нарушитель сети сможет отправить вводящие в заблуждение данные, эксплуатации, администрирование и управление (OA&M – Operations, administration and management) сообщения для сбора информации о сети, о пользователях, о выставлении счетов и так далее. Аналогичным образом, они

могут изменять сетевую информацию, перенаправлять информацию в другие пункты назначения или переполнять сеть, вызывая перегрузку. Предполагается, что этот тип безопасности в достаточной степени решается.

Типичный криптографический модуль содержит в памяти и регистрах состояния функции и алгоритмы шифрования, ключи шифрования (открытый и закрытый), открытый текст и текст шифра.

Традиционно, плохие игроки пытаются получить внутренний доступ к модулю для криптографического механизма или алгоритма и ключам. Для защиты модулей от несанкционированного доступа был разработан стандарт FIPS (Federal Information Processing Standards) 140-2 и его Приложения A, B, C и D, которые определяют четыре уровня безопасности [2]. Ниже приводится краткое описание этих четырех уровней:

– Уровень безопасности 1 (SL-1) — это самый низкий уровень безопасности. Никакие конкретные физические требования не предусмотрены для SL-1. При выполнении физического обслуживания все секретные и закрытые ключи открытого текста и другие критические параметры безопасности (CSP – дополнительный уровень безопасности Content Security Policy) обнуляются, процедурно или автономно;

– Уровень безопасности 2 (SL-2) повышает уровень безопасности LS-1 за счет покрытия пломбами и замками для защиты от несанкционированного доступа на дверь и покрытия;

– Уровень безопасности 3 (SL-3) усиливает LS-2 с помощью механизмов физической защиты и механизмов отчетности. Нарушение ограждения приводит к повреждению модуля. SL-3 требует физически раздельных портов ввода-вывода для шифрованного и обычного текста. Нарушения приводят к обнулению криптографических ключей в модуле.

– Уровень безопасности 4 (SL-4) обеспечивает общую физическую безопасность вокруг криптографического модуля от любого проникновения, доступа к криптографическим ключам и предотвращения внешних условий и изменений окружающей среды. Криптографический модуль содержит либо механизмы защиты от сбоев в условиях окружающей среды, либо механизмы тестирования на сбои в условиях окружающей среды. Попытки удаления или разрушения защитных покрытий должны приводить к самоповреждению.

Безопасность коммуникационной сети, в дополнение к безопасности текста или целостности текста, гарантирует, что сообщения будут доставляться

законным получателям без искажения конфиденциальности, целостности и доступности неавторизованной стороной.

В современных коммуникационных сетях чувствительная пакетная информация поступает на компьютерные узлы, которые могут временно храниться. Узлы обеспечиваются и обслуживаются на месте или удаленно с помощью сетевых управляющих сообщений. Однако, в зависимости от технологии передачи, существуют возможности для атак со стороны образованных злоумышленников. Например:

Зашифрованное сообщение подразумевает безопасность передачи, но только если алгоритм шифрования, который генерирует и распределяет ключи, не может быть взломан. На сегодняшний день несколько алгоритмов и ключей были взломаны с помощью грубой силы (brute force) с использованием суперкомпьютеров или других средств. Таким образом, шифрование сообщения является лишь частью безопасности коммуникационной сети; это называется *безопасностью на информационном уровне*.

Возможно, что физический уровень коммуникационной сети (на канале или узле) прослушивается для подслушивания информации или имитации источника. Таким образом, защита сетевой среды и узлов с помощью механизмов мониторинга и обнаружения называется *безопасностью физического уровня сети*.

Возможно, что злоумышленник заинтересован в том, чтобы нарушить способность сети к передаче данных путем уничтожения сообщений, изменения безопасности и адреса назначения пакетных сообщений, или путем отключения аутентификации и распределения ключей. Это называется *безопасностью на MAC/сетевом уровне*.

Таким образом, интеллектуальная сеть должна быть способна защищать информацию и саму себя, а также иметь стратегии противодействия.

Волоконно-оптические сети DWDM передают огромную емкость информации по 160 оптическим каналам со скоростью 10 или 40 Гбит/с каждый. Волоконно-оптические кабели имеют многокилометровую длину и на протяжении передатчика-приемника они не охраняются. Вредоносные злоумышленники, скорее всего, атакуют оптоволоконную среду в распределительном центре или на оптическом мультиплексоре (OADM), где отдельные волокна легко доступны. Более изощренные злоумышленники могут получить доступ к кабелю и ответвлению волокон. Возможности для

ответвления в центре коммутации наиболее не похожи, если предположить, что центры коммутации физически безопасны.

Открытая оптическая связь (FSO) более безопасна по сравнению с волоконно-оптическими сетями. Связь FSO представляет собой лазерный луч в невидимом спектре (850 нм, 1310 нм или 1550 нм), он находится высоко над землей и поэтому недоступен, а также требует прямой видимости. Таким образом, хотя канал связи хорошо защищен, единственной уязвимой частью сети является кабель, который проходит между приемопередатчиком (лазер/фотодетектор) и узлом или маршрутизатором; этот кабель может быть относительно легко доступен на крышах домов, где установлен приемопередатчик. Однако правильно проложенные кабели в надежных кабелепроводах могут исключить возможность прослушивания кабелей.

Квантовая криптография использует преимущества принципов квантовой механики, таких как принцип неопределенности Гейзенберга [3-6], который утверждает, что зондирование квантовой системы нарушает ее состояние и дает неполную информацию о ней. Согласно этому принципу, в оптической криптографической системе подслушивающее устройство будет нарушать квантовое состояние фотонов. Таким образом, квантовые свойства фотонов, такие как поляризация, фаза, длина волны и запутанность фотонов, используются для генерации секретного случайного криптографического ключа и метода распределения, известного как квантовое распределение ключей (QKD - Quantum key distribution). Первая экспериментальная демонстрация QKD была проведена К.Х. Беннетом и другими [5, 7], проверяя идеи С. Винера. Беннет и др. продемонстрировали, что можно отправить в пункт назначения одновременно два зашифрованных сообщения. Конечный пользователь получает оба сообщения, но, когда одно из них читается, второе автоматически уничтожается; это было названо *квантовой забывчивой передачей*.

В QKD может использоваться один или несколько фотонов. Передача одного фотона обеспечивает лучшую защиту от подслушивания, однако фотоны подвержены взаимодействию с нелинейным диэлектрическим волокном, затуханию, отражениям от разрывов и так далее [6].

И наоборот, множественные фотоны производятся контролируемым образом, они распространяются дальше, но обеспечивают меньшую защиту от подслушивания, поскольку из потока может быть извлечено мало фотонов. Как следствие, в большинстве современных демонстраций используются "хорошо настроенные" квантовые криптографические системы с линейным,

поддерживающим поляризацию и непрерывным волокном, которое поддерживает почти без потерь передачу одного фотона.

Вышеупомянутые стратегии противодействия являются двумя из нескольких возможных сценариев, которые мы изучали в области сетевой безопасности на физическом уровне.

В общем, фотон может находиться в одном из многих состояний поляризации, линейной горизонтальной, линейной вертикальной, линейной под углом, эллиптической, круговой и так далее. В классической теории двоичная система имеет два различных состояния, представленных логическими символами "1" и "0". Квантовая непробиваемая система может находиться в одном из двух состояний, "1" и "0", а также с равной вероятностью в состояниях между ними; то есть состояние системы является суперпозицией всех состояний, "1", "0" и между ними. Только когда состояние системы измеряется, тогда состояние известно и принцип Гейзенберга не действует. Этот неклассический принцип суперпозиции порождает квантовые вычисления, которые основаны на "кубитах" вместо "битов". Если мы рассмотрим поляризационные состояния фотонов [5], то принципы квантовых вычислений применимы к квантовому криминализму, вычислений применимых к квантовой криптографии и к QKD.

ЗАКЛЮЧЕНИЕ

В данной статье представлен расширенный обзор уровней безопасности и уровней безопасности оптических сетей, волоконно-оптических и оптических сетей свободного пространства (FSO). Описаны передовые методы безопасности, такие как квантовая криптография и квантовое распределение ключей.

Определены уязвимые места и обсуждены стратегии противодействия атакам на физическую сеть. Исследования QKD продолжаются в области аутентификации источника и его развертывания в прагматичных оптических сетях.

REFERENCES

1. Fok MP, Wang Z, Deng Y, Prucnal PR. Optical layer security in fiber-optic networks. IEEE T Inf Foren 2011;6(3):725!36.
2. Vahala K, Paiella R, Hunziker G. Ultrafast WDM Logic. IEEE J Sel Toptics Quantum Electron 1997;3(2):698!701.

3. Chan K, Chan CK, Chen LK, Tong F. Demonstration of 20-Gb/s all-optical XOR gate by four-wave mixing in semiconductor optical amplifier with RZ-DPSK modulated inputs. IEEE Photon Technol Lett 2004;16(3):897!9.
4. Wang Z, Fok MP, Prucnal PR. Physical encoding in optical layer security. J Cyber Secur Mobility 2012:83!100.
5. Alam S. and Depole D., "Analysis of Security Threats in Wireless Sensor Network" Int. J. Wir. Mob.Nets., Vol.6, No. 2, (2015), pp. 35-46.
6. Dhamija A. and Dhaka V.," A Novel Cryptographic and Steganographic Approach for Secure Cloud Data Migration" Gr. Comp. Int. Things., 2015 Int. Con. IEEE, (2015)), pp. 346-351.
7. Krishnan S. and Abdullah M.S. " Enhanced Security Audio Steganography by Using Higher Least Significant Bit" J. Adv. Res. Com. Apps., Vol. 2, No.1, (2016), pp. 39-54.