Segurança em Redes Ópticas: Tipos de Ataques e Métodos de Detecção

André Panisson, Ricardo Lemos Vianna, Rodrigo Sanger Alves, Juergen Rochol

Instituto de Informática – Universidade Federal do Rio Grande do Sul (UFRGS)
Caixa Postal 15.064 – 91.501-970 – Porto Alegre – RS – Brazil
{panisson, rvianna, sanger, rochol}@inf.ufrgs.br

Resumo. *Redes ópticas estão sob intenso desenvolvimento e seu uso tem crescido rapidamente. Portanto, avaliar questões de segurança dessa tecnologia torna-se bastante importante. Sendo assim, este trabalho objetiva apresentar métodos de ataque e de que maneira os mesmos podem ser detectados. Por fim, será apresentada, como uma solução de segurança, a técnica de criptografia quântica.*

1. Introdução

Instituições, e.g. universidades e empresas, têm seu funcionamento cada vez mais dependente das infraestruturas de rede. Nesse contexto, tópicos como segurança em sistemas computacionais tornam-se cada vez mais importantes. Assim, alguns estudos foram iniciados no intuito de investigar fatores de segurança em um tipo de rede que se tem destacado pelo rápido crescimento em função da demanda cada vez maior por largura de banda: as redes ópticas [Kartalopoulos 2003]. Novos métodos de ataque e de detecção de ataque surgem, decorrentes das particularidades inerentes às redes ópticas. Além disso, alguns tradicionais métodos devem ser re-estudados.

Este artigo está organizado como segue. A Seção 2 resume os principais tipos de ataque comuns às redes ópticas. Na Seção 3, importantes métodos de detecção são detalhados. Por fim, na Seção 4, são apresentadas as conclusões deste estudo.

2. Tipos de Ataques em Redes Ópticas

De modo geral, os ataques sobre uma rede qualquer podem ser agrupados em seis categorias principais [Nevaste 1999]: análise de tráfego, *eavesdropping* (escuta), *data delay*, negação de serviço, degradação de QoS e *spoofing*. Entretanto, considerando-se o escopo deste trabalho, algumas simplificações podem ser feitas. Análise de tráfego e *eavesdropping* têm características similares e podem ser tratados juntos. Ataques de atraso (*delay attacks*) serão ignorados devido à imunidade oferecida pela tecnologia óptica a este tipo de ataque [Bergman et. al. 1998]. *Spoofing* pode ser prevenido com a adoção de criptografia de dados, que será abordada no final deste trabalho. Negação de serviço pode ser considerado como uma degradação de QoS levada ao extremo, e serão tratados juntos sob o nome "rompimento de serviço". Assim, as seis categorias iniciais de ataque ficam reduzidas a duas: *eavesdropping* e rompimento de serviço.

Para realizar um dos dois tipos de ataques, o atacante necessita de um método. São abordados aqui três métodos em especial [Nevaste 1999, Elsenpeter e Velte 2002]: *In-Band Jamming*, *Out-of-Band Jamming* e Observação Não-Autorizada. Os dois

primeiros são usados para realizar rompimento de serviço, enquanto o último é empregado para realizar *eavesdropping*. No método *In-Band Jamming*, o atacante injeta um sinal para reduzir a capacidade do receptor de interpretar os dados transmitidos. No *Out-of-Band Jamming*, o atacante explora *crosstalk* em componentes ópticos, injetando um sinal de comprimento de onda diferente do usado na banda de comunicação, porém dentro da banda passante do componente. Já na Observação Não-Autorizada, o atacante escuta componentes *crosstalk* de um sinal adjacente, através de um recurso compartilhado, para obter informações deste sinal adjacente.

3. Métodos para Detecção de Ataques

Nesta seção são apresentados métodos para detecção de ataques, e de que forma eles relacionam-se com os tipos de ataques apresentados anteriormente. Algoritmos distribuídos para localização de ataques estão fora do escopo deste trabalho, mas podem ser encontrados, com mais detalhes, em [Bergman et. al. 1998].

3.1. Métodos de Detecção de Energia de Banda

Detecção de energia consiste na medida da energia óptica recebida em uma banda. Pode ser usada para registrar uma mudança de energia em relação ao valor esperado. Pelo fato de um valor medido ser comparado com um valor esperado, uma leve diminuição na energia pode levar um longo tempo para ser detectada. Se a análise estatística for feita sobre grandes números ou sobre um longo período de tempo, então um tempo médio muito longo pode ser necessário para estabelecer com uma certeza razoável que uma mudança na amostra é estatisticamente significante. Mudanças pequenas, mas detectáveis, na energia recebida podem não ser atribuídas a ataques (por exemplo, envelhecimento de componentes ou reparos na fibra), sem assim afetar os sinais de comunicação. Portanto, muitos métodos usam técnicas de detecção de energia sobre um limiar, com os devidos limiares relacionados aos níveis nos quais os serviços de comunicação serão degradados.

No caso de interferências *in-band*, a energia no receptor não será reduzida, mas será aumentada. Um detector de limiar pode verificar claramente um ataque de interferência desse tipo. Uma interferência esporádica poderia aumentar a taxa de erros de forma inaceitável, sem causar um aumento na energia que justifique o disparo de alarme, particularmente se a análise estatística do sinal recebido for claramente determinada. Mesmo que esta análise seja claramente determinada, a natureza esporádica do ataque pode não causar anomalias estatísticas por um longo período de tempo, embora afete a baixa taxa de erros que é necessária para o funcionamento do canal de transmissão.

No caso de interferências *out-of-band*, haverá concorrência pelo ganho do sinal nos amplificadores, e a energia do canal recebido poderá ser reduzida. No entanto, certos ataques desse tipo podem levar a uma degradação no sinal sem uma redução significativa na sua energia. Supondo que um sinal precise atravessar um amplificador EDFA e que haja competição por ganho neste amplificador, o sinal pode não ser adequadamente amplificado.

Técnicas de detecção de energia também têm sido usadas para detectar escutas por perdas de energia. A base para esses tipos de sistemas de segurança é que

apenas uma escuta que drene uma quantidade suficiente de energia do sinal pode apresentar uma detecção satisfatória de tal escuta. Há muitas desvantagens nesse sistema, entre elas o fato de que não consegue detectar um ataque em que um sinal de interferência seja adicionado após a escuta, pois, em contrapartida à perda de energia, haverá um ganho devido à interferência.

3.2. Métodos de Análise do Espectro Óptico

Analisadores espectrais (OSAs) medem o espectro de um sinal óptico, e há muitas implementações desses analisadores. Podem oferecer um diagnóstico mais detalhado do que uma simples detecção de energia. Eles são capazes de detectar mudanças na forma do espectro, mesmo que essa mudança não implique em uma mudança na energia sobre todo o canal. Por exemplo, dois sinais podem ter a mesma energia total, mas espectros diferentes. Um analisador espectral é capaz de distinguir entre dois sinais, enquanto um detector de energia não consegue. Embora analisadores de espectro possam oferecer mais informações que detectores de energia, eles ainda dependem de comparações estatísticas entre amostras. Dessa forma degradações não freqüentes do sinal não serão detectadas ou serão detectadas apenas após um longo período de tempo. Embora ofereçam mais informações que detectores de energia, analisadores espectrais geralmente assumem a existência de alguns efeitos em médio prazo que os fazem mais lentos que outros métodos de detecção.

No caso de interferência *in-band*, um OSA detecta aqueles que afetam de forma significativa o espectro recebido. Fornece mais informação do que detectores de energia, mas para o caso de interferência por *crosstalk*, não fornece mais informações do que um conjunto de detectores de energia específicos para cada extensão de onda.

Já no caso de ataques de interferência *out-of-band*, um OSA será capaz de determinar a fonte do ataque, se a banda analisada pelo OSA for suficientemente larga de forma a abranger a freqüência do ataque.

3.3. Métodos de Sinais Piloto

Sinais piloto são sinais enviados nas mesmas conexões e nodos que os dados de comunicação, porém distinguíveis desses dados. Tem como propósito a detecção de interrupções na transmissão. Sinais piloto são freqüentemente enviados em portadoras diferentes do sinal de transmissão, mas podem também ser distinguidos do *payload* de dados por determinados "*time slots*" (em um sistema TDMA) ou por determinados códigos (em sistemas CDMA). Sinais piloto estão geralmente localizados em portadoras com freqüências entre os canais WDM, assim como fora da banda de transmissão. Se os sinais piloto estão numa freqüência próxima dos canais de transmissão, são geralmente referenciados como sinais "*subcarrier multiplexed*" (SCM). Tais sinais permitem tanto a transmissão de sinalização de rede quanto os sinais pilotos na mesma portadora, pois o sinal não precisa necessariamente ser estático.

Em interferências *out-of-band*, a concorrência por ganho nos amplificadores afeta todos os canais da banda, embora não sejam todos igualmente afetados. Se os sinais piloto usam os mesmos amplificadores que os sinais de dados, então serão afetados da mesma forma. Caso contrário, não é possível detectar ataques desse tipo.

3.4. Métodos que Utilizam OTDRs (Reflectômetros Ópticos no Domínio do Tempo)

OTDRs (*Optical Time Domain Reflectometry*) [Abbade e Caputo 2002] podem ser consideradas aplicações especiais de sinais piloto. Ao invés de analisar um sinal piloto no ponto em que os sinais de comunicação são recebidos, a análise é feita sobre o seu eco. Por causa do freqüente uso de OTDRs e pelo fato destes analisarem o eco do sinal piloto no lugar do sinal em si, OTDRs são considerados em separado, embora compartilhem de muitas características dos sinais piloto. OTDRs são geralmente usados para diagnosticar falhas, curvas (cotovelos) e desperdícios na fibra. Dessa forma, normalmente são mais bem adaptados para detectar ataques que envolvem escutas na fibra. Pelo fato de operarem sobre a reflexão de sinais de volta da fibra, podem dar informação sobre os ataques que estejam acontecendo. Note-se que o sinal usado pelos OTDRs podem ser usados como sinais de supervisão e gerenciamento, podendo também ser submetido à interferência da mesma forma que os sinais piloto. O uso de isoladores ópticos, em conjunção com amplificadores ópticos, é comum, e pode exigir a existência de OTDRs em cada amplificador.

No caso de ataques de interferência *in-band*, parte do sinal de interferência será retornado nas reflexões e se tornará observável. Em redes ramificadas, tais como redes nas quais diferentes canais são demultiplexados em diferentes fibras, secções diferentes podem ser testadas através do envio de diferentes sinais de teste, cada um em um canal diferenciado.

3.5. Novos Métodos para Detecção de Ataques em Redes Ópticas

Alguns métodos novos propostos por Médard, Marquis e Chinn [Médard et. al. 1998] são baseados na noção de que os sinais de entrada e saída de um dispositivo devem ter uma relação matemática que é conhecida pelo sistema de gerenciamento da rede que oferece o serviço. Assim sendo, uma comparação destes sinais será capaz de detectar um ataque se alguma função não produzir uma saída conforme um conjunto conhecido de parâmetros.

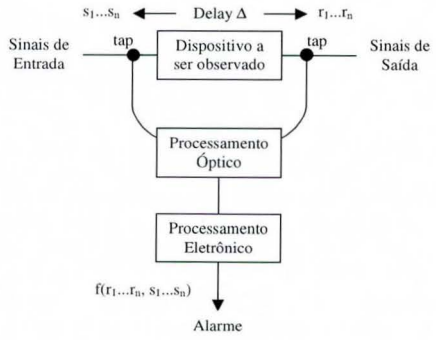

Figura 1. Sistema de detecção de ataques em redes ópticas

O caso geral é mostrado na Figura 1, em que múltiplos sinais de entrada ($s_1...s_n$) são enviados ao dispositivo na esquerda, e os sinais de saída ($r_1...r_n$) aparecem na direita. O dispositivo analisado poderia ser um amplificador óptico em um link ou nodo da fibra, um multiplexador/switch/demultiplexador ou um combinador. O método de detecção insere uma escuta em ambos os pontos de entrada e saída, e consome uma insignificante, porém conhecida porção do sinal para fins de teste. Ambas escutas de entrada e saída são conectadas a uma unidade de processamento óptico opcional. São então transformadas em um sinal elétrico que é processado por uma unidade de processamento eletrônica, cuja saída é função dos sinais de entrada e saída do dispositivo, função essa que faz a medição da operação do dispositivo com respeito a alguns parâmetros. O valor de saída da função determina se será ou não gerado um sinal de alarme. Esta técnica não requer a modificação do dispositivo, pois apenas adiciona um invólucro em torno deste. O alarme poderia estar conectado a um sistema de gerenciamento que poderia processar os alarmes de todos os dispositivos observados.

4. Conclusões

Neste artigo, a questão dos ataques a redes ópticas foi abordada. Inicialmente, apresentou-se uma classificação dos tipos de ataques a redes. Alguns desses foram, então, agrupados, de forma que puderam ser tratados juntos. Outros, como ataques de atraso, os quais não fazem sentido para redes ópticas, não foram tratados. Ataques tipo *spoofing*, que podem ser prevenidos através da adoção de esquemas de criptografia, também estão fora do escopo deste trabalho. Além disso, foram vistos três métodos em especial para realização de ataques dos tipos *eavesdropping* e rompimento de serviço: *In-Band* e *Out-Band Jamming* e Observação Não-Autorizada. Em seguida, diversos métodos para detecção de ataques foram apresentados.

Um campo de pesquisa que poderá colaborar muito na questão da segurança em redes ópticas é a questão da criptografia quântica. Embora não possa impedir ataques do tipo rompimento de serviço, a criptografia quântica pode evitar ataques da categoria *eavesdropping*. Em [Gisin et. al. 2002, Bienfang et. al. 2004], pode-se encontrar uma técnica de gerar chaves criptográficas simétricas de maneira que um atacante escutando a transmissão não poderá descobrir a chave.

Nessa técnica utilizam-se lasers para gerar pulsos individuais de luz, os fótons. A certeza de que os dados não poderão ser lidos é assegurada pelo fato de que a simples tentativa de leitura do fóton, conforme a teoria quântica, causa a destruição deste. Cada fóton pode ser enviado em dois modos de polarização diferentes. Em cada modo, a polarização do fóton em uma das duas orientações possíveis representa o bit 0, e a outra representa o bit 1. O transmissor escolhe randomicamente um modo e uma orientação para cada fóton e o envia em um canal chamado "canal quântico". O receptor escolhe randomicamente um modo de leitura e tenta detectar o fóton. Nesse momento, o transmissor usa um segundo canal para informar ao receptor qual o modo de envio usado para transmitir os fótons. O receptor, então, descarta as medidas feitas no modo incorreto, e informa ao transmissor quais as medidas que foram feitas corretamente (mas não os seus respectivos valores, que formarão a chave). Com isso, o transmissor sabe qual foi a chave gerada no receptor. Nesse ponto, tem-se ambos, transmissor e receptor, com a mesma chave, podendo os mesmos realizar uma comunicação criptografada em um canal qualquer. Se uma tentativa de escuta é feita no canal quântico, uma escolha

randômica de modo de leitura deverá ser feita. A leitura do fóton implica na sua conversão para energia elétrica e, por isso, sua destruição. O atacante deverá gerar um novo fóton para ser enviado ao receptor, mas é impossível saber se o seu modo de leitura estava correto, e, portanto, se o valor lido também estava. Alguns valores serão, então, enviados errados ao receptor, causando diferenças entre as chaves do transmissor e do receptor. Através da comparação de pequenas porções da chave gerada, o transmissor e o receptor percebem que houve escuta no canal quântico, e a chave será descartada.

Por fim, convém ressaltar que a pesquisa a respeito de segurança em redes ópticas deve acompanhar as freqüentes inovações feitas pelos atacantes, além da sofisticação de suas técnicas. Os métodos de detecção de ataque apresentados neste estudo constituem um bom panorama da área, porém as inovações na área de segurança são freqüentes, tanto do ponto de vista de ataque quanto - conseqüentemente - de defesa, reforçando a necessidade de constante atualização.

Referências

Abbade, A. L. R. e Caputo, M. R. C. (2002) "Aplicação do OTDR na Análise de Problemas de Atenuação em Fibras Ópticas: Estudo de Casos", In: Inatel Revista Telecomunicações, Vol. 5, Número 2.

Bergman, R., Médard, M. e Chan, S. (1998) "Distributed Algorithms for Attack Localization in All-Optical Networks", In: The Internet Society's Symposium on Network and Distributed System Security.

Bienfang, J. C., Gross, A. J., Mink, A., Hershman, B. J., Nakassis, A., Tang, X., Lu, R., Su, D. H., Clark, C. W., Williams, C. J., Hagley, E. W. e Wen, J. (2004) "Quantum key distribution with 1.25 Gbps clock synchronization" In: Optics Express, Vol. 12, Issue 9.

Elsenpeter, R. e Velte, T. J., Optical Networking: A Beginner's Guide, McGraw-Hill, 2002.

Gisin, N., Ribordy, G., Tittel, W. e Zbinden, H. (2002) "Quantum cryptography" In: Reviews of Modern Physics, Vol. 74, Issue 4.

Kartalopoulos, S. V., DWDM: Networks, Devices and Technology, IEEE Press, 2003.

Médard, M., Marquis, D. e Chinn, S. R. (1998) "Attack Detection Methods for All-Optical Networks", In: Internet Society's Symposium on Network and Distributed System Security.

Nevaste, K. (1999) "Optical Network Security", Disponível em: http://www.tml.hut.fi/Opinnot/Tik-110.501/1999/papers/optical_netsec/onetsec.html, May.