文章编号：1000-7032(2009)04-0499-04

全光网络中攻击定位和恢复算法的研究与仿真

梁小朋，黄 冰，王 涛，刘联海
（桂林电子科技大学 信息研究室，广西 桂林 541004）

摘要： 分析了全光网络分布式攻击定位算法，构建了全光网络攻击定位与恢复的仿真平台。实验表明，针对单点攻击，对光网络的透明性引起的“攻击泛滥”，能够利用分布式攻击定位算法找到攻击源头，在此基础上，对自动保护倒换和环回两种全光网络进行快速恢复。

关 键 词： 分布式攻击定位；自动保护倒换；环回
中图分类号： TN491 **PACS：** 42.82.-m **PACC：** 4282 **文献标识码：** A

1 引 言

全光网络具有超快的数据传输速率，但也给网络信息安全方面带来一系列新挑战。具体来说，全光网络具有的透明性和大容量性，为恶意用户提供了可趁之机，使业务质量降级或直接导致业务中断。怎么识别和定位攻击，使全光网络中的业务从攻击中迅速恢复过来，这是当前急需解决的问题。本文对 Bergman 等[1]针对网络攻击定位提出的一种新算法——分布式攻击定位算法做了进一步的研究，构建了全光网络攻击定位与恢复的 vc 仿真平台，实现单点攻击源的准确定位，并且对自动保护倒换和环回两种通用型全光网络进行了快速恢复。

2 识别攻击以及攻击定位算法

在全光网络中，激光器、光电转换器、发送器、接收器、光滤波器、光开关、耦合器、光再生器及光放大器等器件是被攻击的对象。我们把这些器件看成是一个个节点，再通过光功率计、光谱分析仪、眼图监视器、BER 监控器和光时域反射计等设备可以检测各个节点是否受到攻击。

攻击的识别与定位有两种控制方式：集中式控制和分布式控制。在集中式控制下，由于所有的控制信息都是由主控节点下发的，各节点的检测结果送到主控节点，由主控节点进行分析和处理，包括在发生攻击的情况下定位攻击源。在分布式控制下，各节点的地位是平等的，各节点对攻击的检测和定位都由自己完成，具有很强的时效性。

分布式攻击定位算法，对单点攻击源来说，各节点只需要使用节点本身和直接上游节点信息。网络中的每个节点都监测其工作是否异常，再根据直接上游节点信息来确定它是攻击源还是其他节点的攻击转移过来的。

如图 1 所示，j 是当前节点，i 是直接上游节点，k 是直接下游节点。设 τ^{means} 是节点检测时间（包含节点检测自身状态的延时加上生成发送给上游或下游状态消息的延时），τ^{proc} 是节点处理时间（包含捕获上游节点的状态消息，并根据这些状态消息和当前节点的状态消息判断当前节点是否是为攻击源的延时），T_{ij} 是传输时间（从节点 i 到节点 j 这段光路的传输延时）。

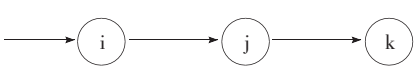

图 1 节点间的连接示意图

Fig. 1 The connection between nodes

在 t 时刻，所有节点都在检测自身的状态，并且把检测到的状态生成节点状态消息，这段时间为 τ^{means}。经过 T_{ij} 时间，直接上游节点 i 的状态消息传到当前节点 j。如果当前节点 j 状态消息为

收稿日期： 2008-10-26；**修订日期：** 2008-11-26
基金项目： 广西自然科学基金（桂科自 0640167）资助项目
作者简介： 梁小朋（1983－），男，江西瑞金人，主要从事全光网络安全的研究。
E-mail：liangxiaopeng315@163.com

正常,经过 τ_j^{proc} 时间就能判定它不是攻击源。如果当前节点 j 状态消息为异常,它需要节点 j 的状态消息和它的直接上游节点 i 的状态消息来判断:若经过 $\tau_i^{means}+T_{ij}$ 时间后,节点 j 没有收到直接上游节点 i 状态消息,则认为节点 j 是攻击源;若节点 j 收到直接上游节点 i 状态消息,则根据直接上游节点状态消息来判断节点 j 是否是攻击源(直接上游节点 i 状态正常,节点 j 就是攻击源;直接上游节点 i 状态异常,节点 j 就不是攻击源)。

基本攻击定位算法的时间关系:

(1)节点完成一次处理的时间 T_j

$$T_j = \max(\tau_i^{means},\tau_j^{means}) + T_{ij} + \tau_j^{proc}$$

(2)网络中两次检测之间的最短时间 T(检测周期)

$$T = \max(T_1,T_2\cdots T_n)$$

其中 $T_1,T_2\cdots T_n$ 为网络中各节点完成一次处理的时间,T 是一个周期时间。

(3)攻击发生后的第 n 个周期攻击传播的距离 L_N

$$L_N = (n\times T - T_0)\times V$$

其中 T_0 为攻击发生时刻时检测周期开始的延时,V 为信息(含攻击信息)在光缆中的传播速度。

攻击发生后的第 n 个周期能检测到的攻击的传播距离 D_N

$$D_N = [(n-1)\times T - T_0 + \max(\tau_i^{means},\tau_j^{means})]\times V$$

攻击传播的极限距离 L_{max},

$$L_{max} = (Q - Q_0)/W$$

其中 Q 为攻击初始强度,Q_0 为能检测到的最小攻击强度,W 为单位距离内攻击衰减的强度。D_N 的范围极限是攻击信号衰减到不能检测设备不能检测为止即 $D_N \leqslant L_{max}$。

3 全光网络攻击定位与恢复的仿真平台

在上述分析的基础上,构建了全光网络攻击定位与恢复的仿真平台,该平台有能够仿真3~15个节点的任意拓扑形状的网络;针对光网络的透明性引起的"攻击泛滥",能够利用分布式攻击定位算法找到攻击源头;能够对攻击传播危害程度和应用攻击定位算法后受攻击的危害程度进行对比评估;并将分布式攻击定位算法用于自动保护倒换和环回网络中,实现网络恢复。

3.1 攻击定位算法仿真

攻击定位算法可分为六个模块:设置光物理层路径模块、设置链路距离模块,配置业务流模块、设置功率模块、循环模拟攻击定位模块、定位报告模块。设置光物理层路径模块可生成一个光物理层上的基本硬件路径;设置链路距离模块可在物理层路径的基础上去设置路径的距离;配置业务流模块可在光物理层路径的基础上设置要传输的业务;设置功率模块可配置攻击源功率、光纤衰减和检测的门限值;循环模拟攻击定位模块可模拟攻击源、攻击传播和定位攻击源。定位报告模块可将以报告的形式来说明定位的过程。

图2是一个有15个节点的实际的网络拓扑图,圆圈表示节点,圆圈里面的数字是节点的编号,实线表示链路,实线上的数字表示实际链路距离(单位:km)。

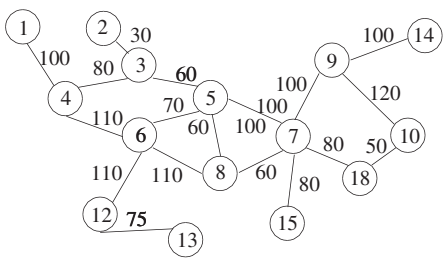

图2 实际网络拓扑图

Fig. 2 The topology of actual network

设置的业务流有8个,分别为{4,6,7,9,14}、{2,3,4,6,8,7,15}、{14,9,10,11,7,5,6,12,13}、{2,3,5,8,7,15}、{1,4,6,5,8,7,11,10,9,14}、{2,3,5,6,8,7,9,10,11}、{2,3,5,7,8,6,12,13}、{2,3,4,6,5,8,7,11,10,9,14},每对括号为一个业务流,括号中的数字是节点的编号,最左边为源节点,最右边为目的节点,业务由左向右逐个传播。攻击源功率、光纤衰减和检测的门限值分别为 -20 ~ -30 dB,3 dB/km, -100 dB(这些数值根据实际设置的参考值,可自行设置)。

运行结果如下:

图3、图4分别表示第一和第二个检测周期的运行结果,从图中可以知道,在一个周期后受攻击源(节点6)的影响,有4个节点异常,同时第一个周期即定位出攻击源;在二个周期后受攻击源(节点6)的影响,有10个节点异常。

定位报告如图5所示,定位报告包含在 τ_i^{means} 结束时刻各个节点的状态和攻击源的定位情况。

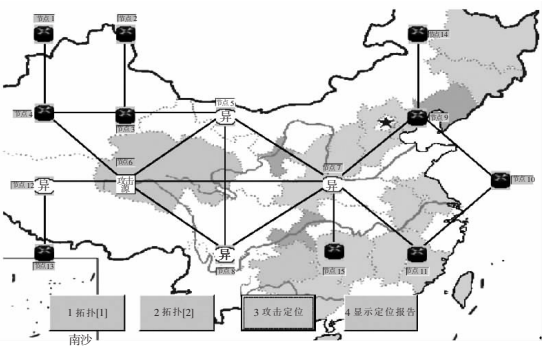

图 3　第一个周期后的运行结果

Fig. 3　Operation results after the first cycle

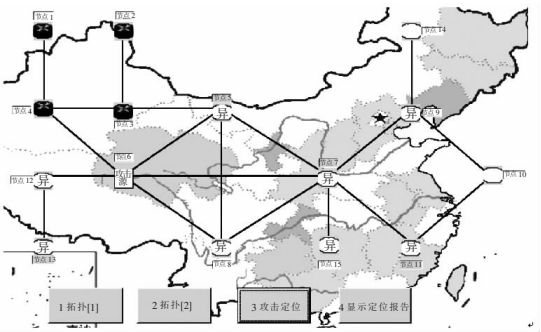

图 4　第二个周期后的运行结果

Fig. 4　Operation results after the second cycle

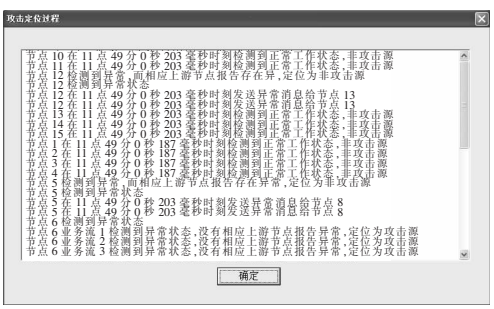

图 5　定位报告

Fig. 5　Localizable report

3.2　恢复算法仿真

自动保护倒换恢复允许网络在节点故障发生时从备份流接受数据。基本攻击定位算法可以用于找出攻击是否发生在主要路径。网络由两条路径构成：主要路径和备份路径（仿真中两条路径可互换）。如果攻击发生于主要路径，将有消息指示该攻击的存在，并在主要路径中传输。目的节点因此将知道上游存在攻击，目的节点的响应将会是去接收备份流。该网络需要两个响应函数：一个用于目的节点，一个用于所有其他节点。以一个小单元为例，运行结果如图 6 所示。从图 6 中所示实线是备用通道，虚线是主通道。节点 1 为源节点，节点 9 为目的节点。

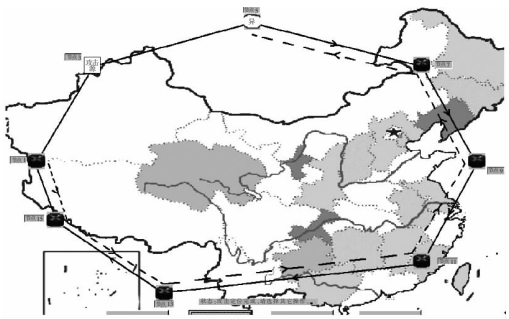

图 6　自动保护倒换恢复

Fig. 6　Restored automatic protection switching

环回恢复由临近攻击源的两个节点完成。如果节点 3 是攻击源，数据流在节点 1 重路由，用备份信道传输。同时节点 5 从备份流接收。这种恢复维护了环的连通性并允许数据到达目的地且不受节点 3 处攻击源的影响。运行结果如图 7 所示。从图 7 中所示实线是备用通道，虚线是主通道。

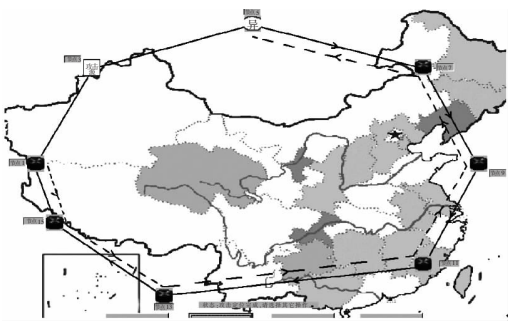

图 7　环回恢复

Fig. 7　Restored loopback

4　结　　论

研究了分布式攻击算法，该算法只需要知道节点及其上游的节点的工作状态，就能确定节点是否为攻击源。在此基础上，构建了全光网络攻击定位与恢复的仿真平台，该平台能在任意拓扑的网络中，根据需要设置物理路径和距离、配置业务流、设置功率和模拟攻击传播等，再根据上述算法迅速地找到攻击源，对受到攻击的自动保护倒换和环回类型网络能自动恢复。但以上算法和仿真都是针对单点攻击，对于多点攻击的情况，算法

还需要进一步的改进。多点攻击问题定位的难点是如何区分两个相邻异常节点中的一个异常节点是受到另一个节点的影响,还是两个节点都是攻击源,这是今后一段时间要研究的问题。

参 考 文 献:

[1] Bergman R, Medard M, Chan S. Distributed algorithms for attack localization in all-optical networks [C]. Network and Distributed System Security Symposium, 1998.

[2] Robert Elsenpeter Toby J Velte. *Optical Networking A Beginner's Guide* [M]. Beijing: Tsinghua University Press, 2003, 375-402.

Research and Simulation on Attack Localization and Restoration in All-optical Networks

LIANG Xiao-peng, HUANG Bing, WANG Tao, LIU Lian-hai

(*Communication Laboratory*, *Guilin University of Electronic Technology*, *Guilin* 541004, *China*)

Abstract: In all-optical networks, distributed algorithms for attack localization was analyzed, and an all-optical network simulation platform was constructed for attack localization and resumption. For a single point of attack, the experiment showed that the distributed algorithm for attack localization can find the source of attacks, which is caused by "rampant attacks" of the transparency of the optical network. On the basis of this, automatic protection switching and loopback are restored quickly.

Key words: distributed algorithms for attack localization; automatic protection switching; loopback

CLC number: TN491 **PACS**: 42.82.-m **PACC**: 4282 **Document code**: A

Received date: 2008-10-26