边界路由器 BGP 协议的脆弱性①

庞 玲

(四川行政学院 计算机系, 成都 610072)

摘 要: 深入地研究了骨干路由器上 BGP 协议的脆弱性, 重点分析了 CXPST 算法的攻击原理, 并提出了改进型的震荡路径选取策略, 从理论上证明了改进型震荡路径选取策略的更优性. 实验测试表明, 利用本文设计的 BGP 协议攻击算法比 CXPST 算法攻击效果更明显, 能够在更短时间内导致运行 BGP 协议的骨干路由器陷入瘫痪.

关键词: BGP 协议; 脆弱性; 路由器; CXPST; DDoS 攻击

Vulnerability of the Border Router BGP Protocol

PANG Ling

(Computer Department, Sichuan Administration Institute, Chengdu 610072, China)

Abstract: This paper has deeply studied the vulnerability of the BGP protocol running in the backbone routers, laid special stress on analysing the CXPST Attacks algorithm, and introduced the improved shock path selection strategies, theoretically proved that the improved shock path selected strategy better. Experimental tests show that the BGP protocol attacked with the designed algorithm is more effective than that of CXPST algorithm, which can result in the backbone routers running with BGP dropping down in less time.

Key words: BGP protocol; vulnerability; routers; CXPST; DDoS attack

1 前言

BGP 协议也即为边界网关协议, 这是一种应用于自治域之间的边界路由协议, 而且运行边界网关协议的路由器一般都是网络上的骨干路由器. 由于骨干路由器在网络上扮演着非常重要的通信角色, 因此针对骨干路由器以及骨干路由器上运行的 BGP 协议安全性研究一直没有停止. BGP 协议作为边界网关路由器运行的最经典的路由协议, 尤其受到人们的重视[1-3], 近年来针对 BGP 协议的安全性分析相关文献有很多, 比如: 胡湘江, 朱培栋, 龚正虎等人设计了一种 BGP 安全机制[4], 通过采用基于 AS 联盟的安全体系结构,使用一种具有分布式认证中心的新的信任模型, 提高了 BGP 协议的安全性. 李琦,吴建平,徐明伟等人充分考虑了安全BGP的目标[5], 提出了 BGP 协议的改进方案, 利用可信计算技术的基础, 采用基于身份的密钥(IBS)算法确保 BGP 协议中身份的真实性, 防止对 BGP 协议的欺骗. 季莉对边界网关协议 BGP 安全性进行了分析[6], 并从认证和签名的角度提出了改进和加强的策略.

尤其是 2011 年有美国明尼苏达大学 Max Schuhard 等发表于国际会议 NDSS2011 的一篇文献中[7], 提出了一种基于 BGP 协议漏动的 CXPST 攻击算法. 这一攻击策略利用 BGP 路由器正常工作过程中路由表更新机制, 通过在网络上制造某些通信链路的时断时续的震荡效应, 导致网络中路由器频繁地更新路由表, 最终当网络上震荡路径数量足够多、震荡的频率足够高, 可以导致网络上所有路由器都处于瘫痪状态. 在该文献中进行实验表明, 如果在互联网上建立一个由 25 万台肉鸡所组成的僵尸网络, 对互联网的关键路径发起拒绝服务攻击, 那么可在 300 秒之内导致骨干路由器的处理延时在 200 分钟以上, 这一现象也就意味着骨干路由器陷入瘫痪状态. 然而这种攻击过程所需要的实现代价比较高, 为了能够更加深入地研究 BGP

① 收稿时间:2012-06-07;收到修改稿时间:2012-07-26

协议的脆弱性, 促使人们对 BGP 协议的安全性进行研究和提高, 本文对 CXPST 攻击算法进行了深入的研究并提出了改进的策略, 更明确地指出了 BGP 协议在应用中的脆弱性.

2　边界路由器BGP协议工作机制

BGP 协议一般指配置于边界路由器上, 当一台路由器配置为 BGP 路由协议后, 该路由器的 BGP 协议会使用 TCP 协议与其他相邻的 BGP 路由器进行通信, 在工作之前, BGP 协议并不会主动地进行 BGP 邻居的发现, BGP 的所有邻居都必须通过手工指定的方式进行配置[8,9]. 当一台运行 BGP 协议的路由器与其他另外一台路由器建立起邻居关系之后, 两台路由器会定期地交换路由信息. 一般路由器与路由器之间会使用 hello 数据包来维持邻居关系. Hello 数据包也被称为是 Keepalive 数据包, 这种数据包每隔 60 秒会发送一次, 邻居路由器收到了 Keepalive 数据包之后就认定其相邻的路由器当前是处于存活状态. 同时, 路由器会设定一个 Holdtime 的时间参数. Holdtime 也即为保持时间, Holdtime 的时间设置一般为 180 秒, 其表达的含义是如果路由器在 180 秒之内没有收到邻居路由器发送过来的 Keepalive 数据包, 则认为当前邻居路由器不属于活动状态, 此时路由器会断开与相邻路由器的链路连接, 并更新路由器上的路由表信息. BGP 路由器在正常工作时, 其 Keepalive 时间和 Holdtime 都可以通过路由器的配置命令来动态进行修改. 当路由器上的这两个时间参数确定之后, 路由器将以这两个时间参数定期地发送数据包维持相互的连接关系, 保证路由器之间通信的正常进行[10].

3　BGP协议的脆弱性分析

3.1 BGP 协议攻击原理

如图 1 所示, 对边界路由器拓扑连接图中的任意一条边 e 用如下公式计算其通信权值.

$$Droute(AB,e)=\sum route(AB,e)$$

其中, $route(AB,e)$ 表示一条给定的从 A 到 B 的路径, 是否经过给定的边 e, 如果该路径经过了边 e, 则 $route(AB,e)$ =1, 否则 $route(AB,e)$ =0.

文献[7]中描述的 BGP 协议的攻击原理是对一个给定的网络, 选取网络的两个节点 A 和 B, 如图 1 所示 A 和 B, 计算 AB 之间的关键路径, 然后以关键路径作为震荡路径, 采用一定的攻击策略, 如文献一中采用 ZMW 攻击算法[11]来实现对关键路径的 DDOS 攻击, 从而导致连接关键路径的路由器侦测到其连接链路上处于时断时续的状态. 因此当两个路由器之间的链路处于断开时, 路由器会自动的更新其路由表, 同时将路由表更新信息发送给其相邻的路由器. 当路由表的更新信息传递到相邻的路由器后, 相邻路由器也将更新其路由表, 同时将更新之后的信息传递给与其相邻的其他路由器, 如此循环往复, 造成路由表更新信息在整个网络中被扩散传递. 在正常的网络应用过程中, BGP 协议的运行环境相对比较稳定, 路由器很少会频繁地连接或断开, 因此 BGP 协议之间的路由更新过程很少发生[12][13]. 然而, 如果攻击者对网络中某些关键路径发起 DDOS 攻击, 则会导致网络中路由器处于频繁更新路由表的状态. 当攻击路径的震荡频率达到一定程度时, 将会在网上叠加产生大量的路由表更新信息, 从而导致路由器无暇处理数据转发任务, 而将所有计算资源都投入到路由表的更新过程中, 最终使得路由器崩溃, 无法提供正常的数据转发功能.

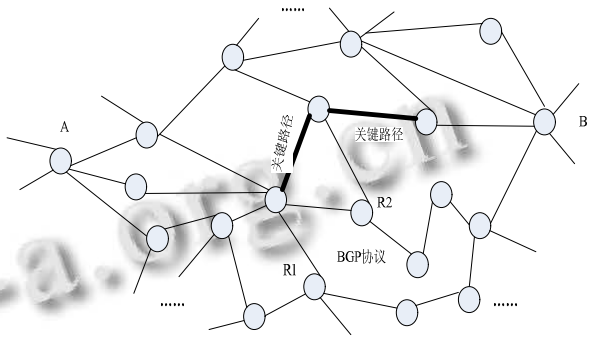

图 1　BGP 协议攻击原理

3.2 改进型振荡攻击路径计算

(1) CXPST 算法震荡路径计算中的问题

定理 1. 直接选取关键路径作为震荡路径不是最佳的方案

证明: 根据前面所述, 对 BGP 协议攻击时的关键路径 e 选取策略可知, 所选取的关键路径 e 是链路 AB 之间多条路径共享度最高的边, 这也意味着有从 A 到 B 的所有路径中, 大部分的数据都将经过 e.

如果选取 e 作为震荡路径, 当网络拓扑中发生路径震荡时, 边 e 周围的其他路由器都将收到路由更新

消息.

当路由器完成了路由表的更新后, 又将向其他路由器扩散路由更新信息.

由于扩散的叠加效应, 一次路径震荡导致路由器上路由表更新次数最多的路由器一定不与边 e 直接相连, 而应该是边周围链路上的路由器. 如图 1 中的 R1, R2.

当关键路径上的路由器由于大量的路由更新信息到达, 而导致路由器陷入瘫痪. 而根据路由扩散的叠加效应, 在关键路径路由器的外围, 必定会存在某些路由器的路由更新计算量更大.

如果产生叠加效应的位置正好在关键路径的路由器上, 则关键路径上的路由器将最先陷入计算瘫痪. 而根据之前对关键路径的计算原则可知, 关键路径是连接 AB 之间共享度最高的边. 由此可见, 直接选取关键路径作为震荡路径不是最佳的方案. 证毕.

(2) 改进震荡路径设计原理

为了更好地设计更优的震荡路径选取策略, 引入了震荡影响因子的概念.

定义 1. 震荡影响因子. 震荡影响因子是指网络拓扑中某段路径发生震荡对当前路由器路径选择的影响程度, 记为 $f(R, path(a,b))$.

若网络上的某段路径发生震荡, 一定会导致路由器路由表更新, 则称该路径的震荡对路由器的影响因子 $f(R, path(a,b))$ =1.

如果发生震荡的路径与某个路由器直接相连, 则该路径的震荡对路由器的影响因子 $f(R, path(a,b))$ =1. 如图 2 所示, 路由器 R3 与 R4 的路径发生震荡, 则对路由器 R3 的影响因子为 1. 如果发生震荡的路径不与当前路由器直接相连, 则该震荡路径对当前路由器的影响因子可能小于 1($f(R, path(a,b))$ <1), 也可能大于或等于 1($f(R, path(a,b))$). 具体的震荡影响因子的计算过程如下:

如图 2 所示, 若对于给定的 AB 之间的网络拓扑, 每个节点都是运行 BGP 协议的边界路由器.

R2 和 R10 之间的路径发生震荡, 所以有 $f(R2, path(R2,R10)) = 1$

由于 R7 有 3 个不同的转发分支, 假设每个分支进行数据转发的代价是均等的, 则 R7 的影响因子由如下公式计算得到:

$$f(R7, path(R2,R10)) = \frac{1}{3} * f(R2, path(R2,R10))$$

同理可计算得到:

$$f(R8, path(R2,R10)) = \frac{1}{4} * f(R7, path(R2,R10))$$

$$f(R1, path(R2,R10)) = \frac{1}{5} * f(R8, path(R2,R10))$$

同时, R2 路由表更新直接也会对 R1 产生影响, 因此有:

$$f(R1, path(R2,R10)) = \frac{1}{5} * f(R2, path(R2,R10))$$

以此类推, 可以得到路径 $path(R2,R10)$ 的震荡, 对路由器 R1 的总影响因子为:

$$Totle(f(R1, path(R2,R10))) = \sum_{i=1}^{5} \frac{1}{5} * f(Ri, path(R2,R10))$$

其中 R_i 代表与路由器 R1 相邻的 5 个路由器.

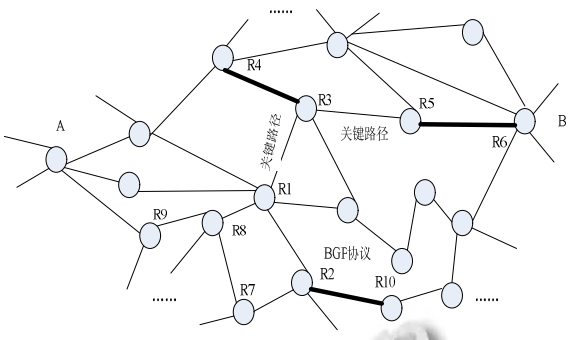

图 2 改进型震荡路径的选取

由于 BGP 协议的扩散效应, 各个路由器更新路由表后, 向其他路由器发送同步更新的数据报不会是同时到达, 而且路由器收到更新包后, 也将逐一进行处理. 因此路由器进行更新路由表的频度取决于震荡路径对路由器总震荡因子. 路由器收到更新数据包后, 会按一定策略进行路由表的更新, 震荡影响因子过小的路由器发送的更新包将被忽略, 只有达到一定阈值的震荡影响因子, 其产生的路由表更新数据包才被接受, 并进行路由表的更新.

因此, 路径 $path(R2,R10)$ 震荡对路由器 R1 的产生的路由表总更新次数为:

$$Totle\_update(Ri) = \sum_{i=1}^{5} Wupdate(f(Ri, path(R2,R10))$$

其中

$$Wupdate(f(Ri, path(R2,R10)) = \begin{cases} 1 & f(Ri, path(R2,R10) \ge \alpha \\ 0 & f(Ri, path(R2,R10) < \alpha \end{cases},$$

由于 R1 是 AB 链路上的关键路径，为了更快速的将 BGP 震荡导致的路由表更新攻击效果展示出来，震荡路径的选取应确保 R1 的路由表更新次数最多，即选取两个相邻的路由器 (Ri, Rj)，使其满足 $\max(Totle(f(R1, path(Ri, Rj))))$ 的路径为最佳震荡路径.

按照这一选取策略，目前对如果快速在一个大规模骨干网络中计算 (Ri, Rj) 的算法尚未研究，不过即便缺乏快速生成 (Ri, Rj) 算法，由于震荡影响因子的总计算量不大，采用穷举的方式也很容易计算得到 (Ri, Rj).

4　仿真实验

针对本文设计的改进型振荡攻击路径计算策略，建立了仿真实验环境，模拟由骨干路由器组成的互联网络的路由更新过程. 本文设计的仿真环境中，建立了一个由 500 个路由器组成的骨干网络，所有路由器都运行 BGP 协议，为了简化问题分析的难度，假设所有路由器的性能都是同等的，所有路由器在路径选择时，只依据拓扑关系进行选择，不涉及路由通信的 QoS 等问题. 选定网络拓扑中关键路径上的一台路由器，进行仿真测试，得到图 3~4 的测试结果.

图 2 给出的震荡路径对路由器 CPU 负荷的影响，为了能够在更短的时间内测量到震荡路径对骨干路由器 CPU 负荷的影响，本文从仿真实验环境中的路由器所组成的拓扑网络中，选取了 24 段路径作为震荡路径，分别用本文设计的算法，从模拟网络拓扑链路中选取 24 段震荡路径，并与 CXPST 选取的 24 段震荡路径进行对比测量. 测量结果如图 3 所示. 从图三可以看出，应用本文设计的算法在实际测量过程中，骨干路由器 CPU 的负荷相对较高，而且在 20 秒的时候，应用本文设计的算法，路由器 CPU 负荷已经基本达到百分之百，而 CXPST 算法所导致的路由器 CPU 负荷只有 86.3%，由此可见，应用本文设计的算法在一个网络拓扑图中选取震荡路径可以在更短时间内导致整个网络上路由器陷入瘫痪.

图 4 给出的是随着震荡路径上震荡频率的改变，而对骨干网络上路由器 CPU 负荷的影响，在测试过程当中，选取震荡路径不同的振荡频率进行测试，振荡频率从每分钟震荡 10 次，到每分钟震荡 60 次不等. 从图四的测量结果可以看出，本文设计的算法在同等的振荡频率下将导致路由器 CPU 的负荷更高，而且图 4 也反应出应用本文设计的算法，骨干路由器上的 CPU 只需要在相对更低的振荡频率下，即将导致路由器 CPU 负荷达到百分之百. 这也说明，应用本文设计的算法，将只需要付出更低的代价就有可能导致整个网络上骨干路由器陷入瘫痪.

从图 3 图 4 的测量结果表明，本文设计的算法在选取正当路径上比 CXPST 算法将更有针对性，所选取的震荡路径在骨干路由器的 BGP 协议进行路由表更新时，将会产生更大的震荡效果. 这也表明应用本文设计的算法，将更容易定位到骨干路由器 BGP 协议的脆弱点.

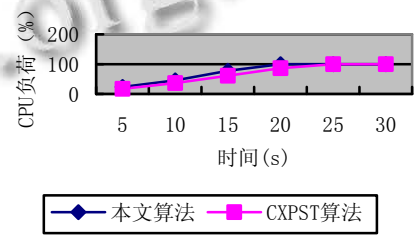

图 3　振荡路径对路由器 CPU 负荷的影响

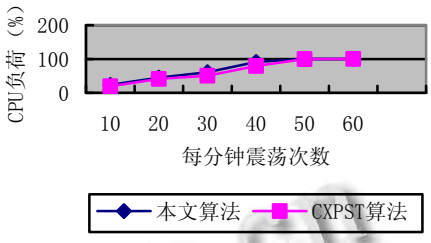

图 4　网络路径振荡频率对路由器性能的影响

5　总结

本文深入地研究了骨干路由器上 BGP 协议的脆弱性，重点分析了 CXPST 算法的攻击原理，并针对 CXPST 算法在设计上的缺陷和不足，提出了改进型的震荡路径选取算法. 经仿真实验测试表明，本文设计的算法将更容易触发 BGP 协议的脆弱性，然而本文进行 BGP 协议脆弱性分析过程中，对网络上骨干路由器的处理性能都进行了统一的处理，认为所有路由器性能上是等价的，然而实际的网络环境中骨干路由器之间的性能是存在差异，路由选择算法要考虑的因素也很多[14]. 因此面对实际的网络环境，如何分析 BGP 协议的脆弱性，还有待于进一步深入的研究.

参考文献

1 赵金晶,朱培栋,周丽涛.域间路由协议 BGP 收敛时间的定

量分析及预测.计算机工程与科学.2007,29(9):56–57.
2 王娜,张建辉,马海龙,汪斌强.基于前缀分配路径长度的 BGP 源自治系统验证机制.电子学报,2009,37(10):2220–2227.
3 Studer A, Perrig A. The Coremelt attack. Proceedings of the European Symposium on Research in Computer Security (ESORICS), Sept. 2009.
4 胡湘江,朱培栋,龚正虎.SE-BGP:一种 BGP 安全机制.软件学报,2008,19(1):167−176.
5 李琦,吴建平,徐明伟,徐恪,张新文.自治系统间的安全路由协议 GesBGP.计算机学报,2009,32(3):506–515.
6 季莉.边界网关协议 BGP 安全性的分析与加强.计算机应用与软件,2007,24(3):39–40.
7 Schuchard M, Mohaisen A, Kune DF, Hopper N, Kim Y, Vasserman EY. Losing Control of the Internet: Using the Data Plane to Attack the Control Plane. 18th Annual Network & Distributed System Security Symposium.6–9 February 2011.http://wenku.baidu.com/view/ab95aa09844769eae009ed49.html
8 于印泉.边界网关路由协议 BGP 在 Internet 中的应用.数据通信,2002,(1):6−10.
9 伍孝金,宋坤,张宏科.基于 IPv6 的 BGP4+路由策略的研究与实现.计算机工程与设计,2007,28(17):4161−4164.
10 Wang F, Mao ZM, Wang J, Gao L, Bush R. A measurement study on the impact of routing events on end-to-end Internet path performance. SIGCOMM Comput. Commun.Rev., 2006,36(4):375–386.
11 Zhang Y, Mao ZM, Wang J. Low-rate TCP-targeted DoS attack disrupts Internet routing. Proc. of the Network and Distributed System Security Symposium (NDSS), 2007.
12 Sriram K, Montgomery D, Borchert O, Kim O, Kuhn DR. Study of BGP peering session attacks and their impacts on routing performance. IEEE Journal on Selected Areas in Communications, 2006,24(10):1901−1915.
13 喻卫,蔡开裕,朱培栋.BGP 安全机制的研究.计算机工程与应用,2006,42(5):113−116.
14 Sinclair G, Nunnery C, Kang BB. The Waledac protocol: The how and why. Proc. the IEEE International Conference on Malicious and Unwanted Software (MALWARE). 2009,10: 69–77.

(上接第 97 页)

3 结语

本文设计了基于投影的二值图像处理算法并应用于二值化阈值的选取、文档边框的自动辨识和图像污点的自动提取等方面，取得了良好的使用效果，该算法的时间复杂度和空间复杂度较低，是一种较为实用的二值图像快速处理算法，可推广应用于历史图纸的矢量化、栅格图像的矢量化等领域.

参考文献

1 Zhao YQ, Yu DM, Wang YQ. A method of automatic threshold selection in calibration plate image binarization. Modern Manufacturing Enginerring, 2011,4: 99–102.
2 Li HL, Lan MH, Zhang SJ, Yang L. Random Clipping of Curves in Rectangular windows Based on the Projection Method. Journal of Yunnan University of Nationalities, 2011,20:132−135.
3 Liu ZL, Zhou H, Yu L, Min LS. Real-time Instrument Character Recognition System Based on Projective matrix Method. Instutment Technique and Sensor, 2008,8:98−101.
4 Ma RN, Chen TP. Recurrent Neurul Network Model Based on Projcetive Operator and Application in Optimitalion Problem. Appllical Mathmetics and Mechanics, 2006,27:484−494.
5 Wu JP, Yang ZX, Han D, Bai ZF, Su YT. 2D Barcode Image Binarization Based on Wavelet and Ostu Method. Computer Enginerring, 2010,36:190−192.
6 Ostu N. A threshold selection method from gray-level Histograms. IEEE Trans. on System, Man and Cybemetics, 1979, 6: 62−66.
7 Zhou YJ, Wang X, Su X, Yao ZL, Yao CZ. Research on Gray Projcetion Algorithm for Image Stabilization. Ordnance Industry Automation, 2009,28:88−93.
8 Zhou L. Application of projective operator in variance analysis models. Journal of china textile university, 1991,17: 199–208.
9 Li SW, Wang G. Otsu Binarization Application in License Plate Location. Journal of Shunde Polytechnic, 2011,9:2−5.