改进的一致性哈希算法及应用

方 堃[1] 武小年[1,2]

（1.桂林电子科技大学信息与通信学院，广西 桂林 541004；
2.广西无线宽带通信与信号处理重点实验室，广西 桂林 541004）

【摘 要】针对分布式入侵检测中的数据分割问题，给出一种改进的一致性哈希算法。该算法针对采集的数据包，通过 TCP 流重组建立 TCP 数据链，保证数据流的完整性；再通过结点的分组对一致性哈希算法进行改进，并实现组间和组内的数据分配，减少虚拟结点数量；对结点的负载均衡检测和调整策略，改善了系统的负载均衡性。仿真测试结果表明该算法具有较好的负载均衡性。

【关键词】分布式入侵检测；TCP 流重组；一致性哈希算法；负载均衡
【中图分类号】TP393 【文献标识码】A 【文章编号】1008-1151(2015)04-0005-03

Improved consistent hash algorithm and application

Abstract: Aiming at data segmentation problem in distributed intrusion detection, this paper proposes an improved consistent hash algorithm to solve this problem. The algorithm uses TCP stream reassembly technology to rebuild TCP links to ensure data integrity; then divided nodes into different group to improve the consistent hash algorithm. Through the improved consistent hash algorithm, the data can be divided in node and the number of required virtual node is reduced; Load balancing detection of node and adjustment strategy to improve the load balance of the system. The simulation results show that the algorithm has better load balance.

Key words: Distributed Intrusion Detection;TCP stream reassembly;Consistent hash;Load balancing

1 引言

随着网络带宽的不断增大，网络速度的不断提高，传统的基于单主机的入侵检测系统已经很难满足大规模网络高效检测的需求。分布式入侵检测系统是解决高速网络环境下入侵检测效率低下问题的解决方案之一。现今，提升分布式入侵检测系统的性能面对许多难题。首先，数据的完整性对入侵检测系统检测准确率的提升至关重要，因此如何保持数据的完整性是对分布式系统中数据分割算法提出的重大挑战；其次，分布式系统中可能会产生添加或删除结点的情况，此时若采用传统求模运算的哈希函数，则必须重新分配数据，然而在入侵检测中有时需要与历史信息结合来准确判断出攻击行为，此时将产生大量的数据迁移，降低整个系统性能；最后，均衡的保持每个结点的负载，使各个结点发挥出最大性能，也是提升分布式入侵检测系统的关键。因此，实现分布式入侵检测的关键在于数据分割算法。

一个良好的面向分布式入侵检测的数据分割算法应当满足以下三个特征：（1）有效性，即每个数据分片应能准确检测出攻击行为；（2）均衡性，即每一个分片应使各分布式结点负载均衡；（3）简单性，即分割算法简单、高效。文献[1]提出动态最小负载优先算法，将数据优先分配给负载最轻的结点。文献[2]中加入了数据预过滤和缓冲聚类，将检测结点的一部分功能转移到分割模块中，降低了后续模块的处理压力。文献[3]提出的随意分割集中学习的方法，此种算法满足了分割算法的简单性和负载均衡性，但后续的检测较为复杂，不利于实时网络入侵检测的实施。文献[4]综合考虑了影响各结点负载均衡性的因素，优先将数据分配给负载最轻的结点，实现了负载均衡性，然而并没有考虑到数据包之间的联系，破坏了数据的完整性。文献[5]提出基于流粒度的负载均衡算法，以会话流为单位分发数据包，保持数据的完整性。

本文基于一致性哈希算法，给出一种改进的算法，并用于分布式入侵检测的数据分割，该算法针对采集的数据包，通过维护 TCP 连接记录并重组 TCP 数据链，保持数据流的完整性；再通过改进的一致性哈希算法，减小结点间数据的迁移量，同时通过负载均衡策略维持结点间的负载均衡。

2 改进的一致性哈希数据分割方法

在分布式入侵检测中，数据分割的优劣一直是制约分布式入侵检测系统性能的瓶颈。首先，若以单一数据包为最小

【收稿日期】2015-02-10
【基金项目】广西自然科学基金(2012GXNSFAA053224)和广西无线宽带通信与信号处理重点实验室 2014 年开放基金项目(GXKL0614110)资助。
【作者简介】方堃（1990－）男，湖北武汉人，桂林电子科技大学信息与通信学院硕士研究生，研究方向为信息安全。
【通讯作者】武小年（1972－），男，湖北监利人，桂林电子科技大学副教授，研究方向为信息安全，分布式计算。

检测单元，不关心数据包的状态信息，将相互关联的数据包分配到结点，会导致许多攻击行为无法检测出；其次，为了准确检测出攻击行为，有时还需获取历史告警记录。若采用传统哈希函数，当分布式系统中有结点的添加和删除时，将导致整个哈希函数重新分布，为了保证历史记录的准确性，需要迁移大量的历史告警信息，为系统增加负担；最后，若分割算法不能实现负载均衡，则无法充分发挥各结点的计算性能，导致系统整体陷入瓶颈。

针对以上问题，本文首先采用 TCP 流重组技术，以会话流为最小单元保持数据的完整性。TCP 协议在网络中进行传输的时候，由于经过不同的路由，在到达的时间与顺序上会产生混乱，因此要提取出数据流中的 TCP 包进行重组才能还原成一个完整的数据链。为保证将海量的网络数据分割成一个个完整的数据子集，在数据重组时，计算数据包的哈希值。一条 TCP 连接可以由四元组<源 IP 地址，源端口，目的 IP 地址，目的端口>唯一确定，因此，可以通过哈希函数计算四元组的哈希值，作为此连接的唯一标识，结合报文中的连接序号就可以实现正确的 TCP 流重组。针对重组形成的一个个 TCP 流链，进一步采用改进的一致性哈希算法，将不同的 TCP 流链分配到不同的结点，实现数据的分割。

2.1 改进的一致性哈希算法

一致性哈希算法是实际结点对应的虚拟结点映射到 $0 \sim 2^{32}$ 的环上，数据求取哈希值后同样映射到该环上，并按顺时针方向查找与之最接近的虚拟结点，通过虚拟结点与实际结点之间的映射关系将数据分布到真实结点。当有新结点加入或旧结点退出时，仅影响顺时针方向的下一个结点的数据，减少数据的迁移量。

然而传统一致性哈希算法主要针对同构主机，当两个结点的性能相差过大时，需要引入大量的虚拟结点，从而导致虚拟结点需要的存储空间增加和查找速度的降低。假设结点 i 的计算能力为 a_i，由文献[6]得知，每台主机引入的虚拟设备为 $klog|N|$，其中 k 为常数，N 为设备总数。若结点 i 的计算能力为 a_i，计算能力最低结点的计算能力为 a_{min}，则传统一致性哈希函数所需要分配的虚拟结点个数为:

$$\sum_{i=0}^{N} \frac{a_i}{a_{\min}} k \log|N| \qquad (1)$$

当 a_i/a_{min} 的值很大时，将引入大量的虚拟结点，降低整个一致性哈希函数性能。

本文改进算法中，将计算能力相差不大的结点分为一组，组间按照各组结点计算能力的大小比例分割整个哈希值的值域，数据先分配到不同的组中，在组内采用一致性哈希算法，再将数据分配到不同的结点上。由于组内结点计算能力相差不大，因此可以采用均匀分配的方式。采用此方法可以解决异构主机引入虚拟结点过多的问题。假设结点共分为 p 组，组 i 中有 n_i 个结点，由于结点计算能力相差不大，则每组中引入的虚拟结点总数为 $n_iklog|N|$，整个分割系统引入总结点数为：

$$\sum_{i=0}^{p} n_i k \log|N| \qquad (2)$$

当结点计算能力相差很大时，式（1）的值远远大于式（2）的值。

2.2 负载均衡策略

在传统一致性哈希算法中，数据的分配是由概率决定的，因此在容易产生负载不均衡。针对该问题，本文基于上述的改进一致性哈希算法，进一步进行负载均衡调整。系统周期性进行结点负载情况检查，并根据不同组结点数据处理能力不同，设定不同的负载均衡调整门限，当负载不均衡程度超过门限时，进行结点的负载均衡调整。

假设组 i 的权重为 c_i，表示结点的计算能力，计算能力越强的组 c_i 的值越大，计算能力最低的一组权重为 c_{min}，其中 p 为结点组的个数。组 i 负载均衡调整门限为 $Threshold_i$,计算能力最低一组的负载均衡调整门限为 $Threshold_{min}$ 则有：

$$Threshold_i = \frac{c_i}{c_{\min}} Threshoid_{\min} \qquad (3)$$

设组内负载最轻结点负载为 L_{min}，负载最重结点负载为 L_{max}，负载居中结点为 L_{mid}，若类 i 中 L_{max}-L_{mid}>$Threshold_i$，则进行负载过重调整，减少 L_{max} 对应结点的虚拟结点，同时将分配到该结点的数据产生的 T 时间内的告警信息迁移到顺时针方向的下一个结点，并清空该虚拟结点的告警信息。同理，若组 i 中 L_{mid}-L_{min}>$Threshold_i$，进行负载过轻调整，增加 L_{min} 对应的虚拟结点个数，同时将下一结点中的 T 时间内部分告警信息迁移到新的结点中，并清空旧节中迁移部分的告警信息。

负载均衡调整将有效提升一致性哈希算法负载均衡性。使调整后的结点负载接近负载中间结点。同时，检测攻击行为并不需要太长时间的历史记录，因此结点告警信息的迁移量很小，并不会给系统增添过重的负担。

3 实验仿真

3.1 实验环境

本文采用 C 语言实现了网络数据抓包、TCP 流重组，以及分组一致性哈希算法和负载均衡调整算法，并对该算法进行了测试。仿真测试主要测试算法改进后的负载均衡情况。仿真测试网络环境为实验室局域网通过 100M 交换机连接到校园网，并连接互联网。模拟设置了 15 个结点，分为 3 组，每组 5 个结点；各组中结点计算能力分别分布在 1000,3000,6000 附近区间；设置计算能力最低的一组的虚拟结点数为 20。

3.2 实验结果与分析

3.2.1 组间负载均衡实验

由于各组分配的数据量与各组计算能力成正比，若各组负载均衡则该组中处理数据的总量比该组计算能力的值应大致相同。这个值定义为组间相对数据量。各组组间相对数据量差值越小，说明组间负载均衡性越好。均方误差能较好的

反应数据之间的离散程度，均方误差越小说明数据之间的离散程度越低。因此本文采用组间相对数据量的均方误差作为评价组间负载均衡的评价指标，并将本文改进算法与传统一致性哈希函数进行对比测试。实验结果如图 1 所示。

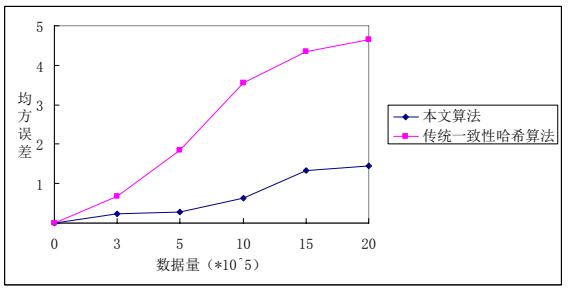

图 1　组间相对数据量均方误差对比图

由图 1 可以看出，本文改进算法中各组组间数据量均方误差远小于传统一致性哈希算法，其原因在于本文算法将数据按照相对权重值的比例均匀分布到各组结点，组间负载性能良好，充分发挥结点的计算能力。

3.2.2　组内负载均衡实验

本实验将本文算法与传统哈希分割算法、传统一致性哈希算法进行对比测试。对比的两种算法将计算能力相同的结点视为一组，同时取第二组结点在不同的数据量下进行负载均衡性测试。实验引入文献[7]中提出的负载均衡度作为评价指标。负载均衡度越小，说明负载均衡性能越好。实验结果如图 2 所示。

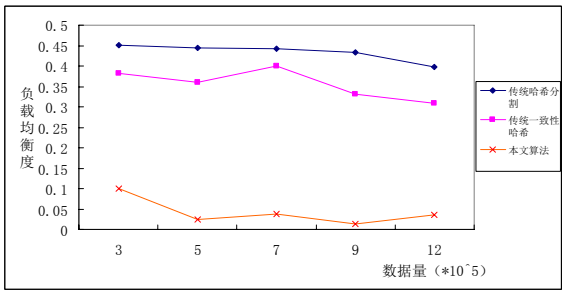

图 2　负载均衡度对比图

由上图可以观察到，由于传统算法没有加入动态调整策略，当局部流量增大时，将导致严重的负载不均衡现象，此种情况需要经过较长时间的调整，才能略有改善。本文算法进行负载均衡调整后，负载均衡性能良好，且波动范围很小，基本实现组内各结点负载均衡。

4　结束语

近年来网络安全形势日趋严峻，分布式入侵检测技术成为维护网络安全的有效手段，分割算法又是影响分布式入侵检测系统性能的关键因素。本文给出改进的一致性哈希算法，并应用于分布式入侵检测中进行数据分割。算法基于对采集数据的 TCP 流重组，并采用分组方法进行结点分组并实现组间和组内的数据分配，减少虚拟结点数量，并通过对结点的负载均衡检测和调整，改善了系统的负载均衡性。

【参考文献】

[1] 李信满,赵大哲,赵宏,等.基于应用的高速网络入侵检测系统研究[J].通信学报,2002,23(9):1-7.

[2] Xinidis K,Charitakis I,Antonatos S, et al. An active splitter architecture for intrusion detection and prevention[J]. Dependable and Secure Computing, IEEE Transactions on,2006, 3(1): 31-44.

[3] 刘衍珩,田大新,余雪岗,等.基于分布式学习的大规模网络入侵检测算法[J].软件学报,2008,19(4): 993-1003.

[4] Jiang W, Song H, Dai Y. Real-time intrusion detection for high-speed networks[J].Computers & security,2005,24(4): 287-294.

[5] 高明.高速网络入侵检测负载均衡机制研究[D].武汉:华中科技大学,2009.

[6] Karger D,Lehman E, Leighton T, et al. Consistent hashing and random trees:Distributed caching protocols for relieving hot spots on the World Wide Web[C]//Proceedings of the twenty-ninth annual ACM symposium on Theory of computing. ACM,1997: 654-663.

[7] 陈一骄,卢锡城,时向泉,等.一种面向会话的自适应负载均衡算法[J].软件学报,2008,19(7):1828-1836.