可重构网络中自适应入侵检测修复算法研究

王 超[1],李永新[2]
(1. 南阳理工学院 软件学院,河南 南阳 473004;
2. 南阳农业职业学院 计算机系,河南 南阳 473061)

摘 要:随着越来越多实时应用程序的出现,计算机网络也面临着诸多挑战,如何有效防御入侵者的攻击已成为亟待解决的问题之一。为此,文中提出了一种在可重构网络环境下进行入侵检测和修复的算法。该算法既能够主动实时检测由入侵者删除节点所造成的网络中断,又能够在路径中断后及时采用基于度数的自适应修复算法来进行修复,以保持网络的连通性。实验表明该算法不仅检测延迟低,而且节点度数的增加和信令开销较小,能够较好地满足可重构网络的实时性需求。

关键词:可重构;入侵检测;修复;实时
中图分类号:TP393.01 **文献标识码**:A **文章编号**:1673-629X(2014)03-0130-04
doi:10.3969/j.issn.1673-629X.2014.03.033

Research of a Self-adaptive Intrusion Detection and Healing Algorithm in Reconfigurable Network

WANG Chao[1], LI Yong-xin[2]
(1. School of Software, Nanyang Institute of Technology, Nanyang 473004, China;
2. Department of Computer Science, Nanyang Agricultural Vocational College, Nanyang 473061, China)

Abstract: As more and more real-time applications emerged, computer network faces many challenges, how to defend attack from intruders efficiently is one of the problems need to be solved. Therefore, an intrusion detection and healing algorithm in reconfigurable networks is proposed. The algorithm can detect outage produced by deleting node actively and timely, and adopt a degree-based self-adaptive healing algorithm to restore the network after path outage, in order to keep connectivity. The experiment shows that the detection delay of this algorithm is lower, and degree increase of the node as well as signaling overhead is smaller than other algorithms, it satisfies the real-time requirements of the reconfigurable networks well.

Key words: reconfigurable; intrusion detection; healing; real-time

0 引 言

网络互联已经变成了现代计算机系统中最主要的部分。传统意义上的网络接口只是一种简单的设备,它用来在网络和操作系统之间转发原始数据,但是随着网络服务器架构的扩展,其功能也在发生着变化。此外,越来越多的嵌入式应用程序具有实时性需求,为了满足这些需求,互联网络要对此提供支持。对于某些无线应用程序来说,实时性需求会随着带宽、工作负载以及操作模式的变化而变化,这就对当前的网络系统提出了更高的要求。可重构网络的出现,使得这些问题迎刃而解。它能够根据当前所运行的应用程序的需求,自动调整网络中的各种参数,以使网络利用率达到最优化[1]。

可重构网络就是由多个芯片互连起来的包交换网络[2],每个芯片中包含有大量的处理器以及可修改的固件。传统意义上的硬件专门用来执行某种特定的计算,具有快速和高效的特点,但一旦设计完成便不能更改,除非进行全新的设计,而这又会造成财力和物力资源的开销增大。而软件则是通过执行一系列的指令来进行计算,只要修改指令便可进行不同类型的计算,具有相当大的灵活性,但是指令在执行过程中都需要先从内存读出,然后经过解码编译才能够运行,这会产生

收稿日期:2013-04-24 **修回日期**:2013-07-27 **网络出版时间**:2013-11-29
基金项目:河南省基础与前沿技术研究计划项目(122300410258);河南省重点攻关项目(112102210408)
作者简介:王 超(1986-),男,河南南阳人,讲师,研究方向为下一代网络、软件工程;李永新,高级讲师,研究方向为网络安全与计算机应用。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20131129.0946.036.html

比较高的开销。可重构网络的出现,就是为了在硬件和软件之间找到一个平衡点,既能使两者的优点得到最大程度的利用,又把弊端所带来的影响减小到最低。可重构网络的一个主要特征就是运行时重构(Run Time Reconfigurable,RTR),指的是通过修改芯片中的固件和 FPGA 硬件来为不同的应用程序构建不同的网络模型,进而研究该网络中的行为特征。

可重构网络的另外一个特征就是灵活性[3],即可以动态地添加边,以此来更改网络的拓扑结构。P2P 网络、覆盖网络、无线 Ad-hoc 网络以及社交网络都属于这种类型。利用这种特性,可以在网络链路失效或者遭受攻击时进行自我修复。文中根据这一特性,提出了一种自适应入侵检测修复算法,通过构建模型并进行仿真实验,表明了该算法能够维护网络连通性,同时使节点的度数增加幅度较小,另外修复过程中的延迟和带宽消耗较少,能够满足实时性需求。

1　相关工作

到目前为止,很多学者都对网络受到攻击后如何自我修复进行了研究。文献[4]提出了在网络中增加额外的存储空间并在受到入侵时重新选择路由的策略来进行修复。Medard M 等人在文献[5]中提出了一种构建冗余树的方法,以便在入侵者删除网络节点或者边时备份路由。Anderson D 等人在文献[6]中将某些现有的网络节点修改为弹性覆盖网络(Resilient Overlay Network,RON)节点,以检测链路失效并根据具体情况重新路由。在文献[7]中,通过增加冗余组件来使网络拓扑结构具有足够多的冗余性,发生入侵时不会影响到系统的整体性能。但这些方法都假设网络拓扑是固定不变的。文献[8]中,Iching Boman,Jared Saia 等人提出了一种直线算法,该算法在入侵者删除节点后,将被删除节点的邻居按照直线重新连接,直线的两个端点是所有邻居节点中权值最大的节点。该算法确保了网络受到攻击后的连通性,同时使节点的度数增加不超过 $O(\log n)$。但是,该算法假定网络是不可扩展的,另外在修复过程中需要交互的信令数量超过了 $O(n)$。除此之外,所有这些方法都没有考虑入侵的检测,即何时发现网络中断。因为修复算法只能在网络发生中断之后的一小段时间内进行,否则在入侵者删除其他节点之后修复算法便不能够保证网络的连通性。

为此,文中提出了一种自适应入侵检测修复算法,它不仅能够实时检测网络的链路状态,还能在链路失效后立即采用位置感知的基于节点度数的自我修复算法(Locality-aware Degree-based Self Healing Algorithm,LDSHA)来确保网络的正常运行。

2　入侵检测修复算法概述

假定网络的初始状态是具有 N 个节点的连通图,每个节点不仅了解自己的邻居节点信息,还知道邻居节点的邻居节点相关信息(Neighbor of Neighbor,NoN)。也就是说,对于节点 x,y 和 z 来说,x 是 y 的邻居节点,y 是 z 的邻居节点,那么 x 不仅知道 y 的相关信息,还知道 z 的信息。假定入侵者已经对网络拓扑结构非常熟悉,每次只删除一个节点。

2.1　入侵检测算法

在该网络中,每个节点自身都维护一个性能数据库[6],其中保存了相关的性能度量标准,如节点度数、链路延迟、吞吐量以及丢包数等等。节点周期性地与邻居节点交换彼此的性能参数信息,以使性能数据库中的数据实时更新。同时,每个节点进行入侵检测,以确定其与邻居节点之间的链路是否中断。该入侵检测算法使用一种主动探寻机制来实现。正常情况下,节点 A 按照 PROBE_INTERVAL 的时间间隔向其邻居节点 B 发送探寻消息 PROBE,如果两个节点之间的链路正常,那么 A 每次发送探寻消息之后就会收到来自 B 的回应消息,如果 A 在每次发送 PROBE 后没有收到 B 的回应,接下来节点 A 就开始以 PROBE_TIMEOUT 的频率来向 B 发送 FAST_PROBE 消息,若 A 发送的 FAST_PROBE 消息数量超过了 OUTAGE_THRESH,节点 B 仍然没有回应,此时 A 就认为和 B 之间的链路中断,然后将此信息保存到性能数据库中并通知邻居节点。在该算法中,PROBE_TIMEOUT<PROBE_INTERVAL。该算法的描述如下:

```
While(链路正常)
{A sends PROBE to B every PROBE_INTERVAL seconds;
if (The edge between A and B is normal)
B sends response to A;
else if (A receives no response from B)
{ A sends FAST_PROBE message to B every PROBE_TIMEOUT seconds;
if (the number of FAST_PROBE exceeds OUTAGE_THRESH and A receives no response)
the edge between A and B is deemed dead or outage;
A save this outage information in the performance database and inform its neighbor nodes;
}
}
```

2.2　LDSHA

在描述 LDSHA 之前,首先给出一些定义。在某一特定时刻,可重构网络定义为 $G(V,E)$[9]。E' 是发生中断后由算法添加到网络中的边($E' \subseteq E$)。$G' = (V,E')$,其中 G' 是一个森林。$N(v,G)$ 是 G 中顶点 v 的邻居节点集,$N(v,G')$ 是 G' 中顶点 v 的邻居节点

集,$\delta(v)$是顶点 v 增加的度数。

当入侵者删除节点 v 时,根据图 G 中 v 的邻居节点的 ID 来进行分区。从每个分区中选择一个有代表性的节点(通常是 ID 最小的节点)组成一个唯一的邻居节点集 $UN(v,G)$,在该集合中每个节点的 ID 都是唯一的。$UN(v,G)\cap N(v,G')=\varnothing$ 并且 $UN(v,G)\cup N(v,G')\subseteq N(v,G)$。

该算法的描述如下:

对于一个给定的网络 $G(V,E)$,为每个节点随机分配一个[0,1]之间的 ID。

While(true)

{ if (a vertex v is deleted)

将 $UN(v,G)\cup N(v,G')$中的节点重新连接到一个完全二叉树中,按照节点 δ 值从小到大的顺序自左至右、自上而下映射到完全二叉树中;

将 $UN(v,G)\cup N(v,G')$中节点的最小 ID 分配到新生成的完全二叉树中

}

经过证明,该算法在网络受到攻击中断后仍能保持连接,并且在修复后没有节点过载,节点度数仅仅增加了 $O(\log n)$,所经历的延时和交换的信息数也只有 $\log n$。此外,该算法是完全分布式的。

3 实 验

为了比较不同修复算法的性能,分别选取不同的入侵策略,并对修复算法在节点度数的增加、延迟时间以及信令开销等方面进行了实验。

实验在 NS 仿真平台中[10]进行。此外,根据 Barabasi 所提出的优先连接模型,该实验所采用的网络是随机生成的图。对于每个图来说,分别选取不同的入侵和修复策略,然后对不同策略的性能(节点增加的度数、延迟以及信令开销)进行比较分析。

假定入侵者的目的是通过使网络节点过载来破坏网络。一种入侵策略是删除具有最大度数的节点,叫做 MaxNodeStrategy(MNS)。另外,在网络中度数最大的节点通常受到保护或者对入侵具有免疫性,针对这种情况,NeighborofMaxStrategy(NMS)持续删除网络中度数最大节点的邻居节点,以此来达到入侵网络的目的。

该实验采取的修复策略如下:

(1)二叉图修复策略[9](Binary Graph Healing Strategy,BGHS):入侵者删除节点后,将被删除节点的邻居节点重新连接到二叉图中,在修复过程中,新增加的边有可能在图中引起环。该算法是最简单的算法,因为它试图增加更多的边来维护中断网络的连通性。

(2)二叉树修复算法(Binary Tree Healing Algorithm,BTHA):入侵者删除节点后,将被删除节点的邻居节点重新连接到一个二叉树中,修复后的网络拓扑是一个森林,这主要是通过为每个邻居节点随机分配一个[0,1]之间的随机 ID 来实现的。该算法虽然不会在图中引入环,但是没有考虑在修复过程中节点度数的增加[11]。

(3)LDSHA。

由于 MNS 不具有代表性,该实验采用 NMS[12]。首先是节点度数的增加。图 1 显示了 LDSHA 节点度数的增加比其他两种算法少,与之前推导的理论结果一致。

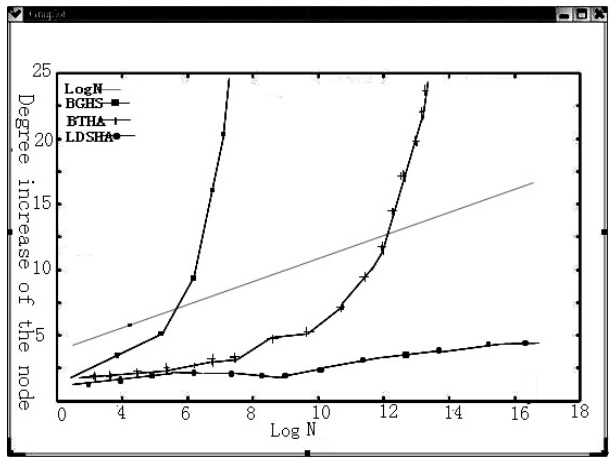

图 1 LDSHA 和其他修复策略关于节点度数增加的比较

因为在该网络中,为每个节点随机分配了一个[0,1]之间的 ID,据此对文中所提出的入侵检测算法进行了实验,结果如图 2 所示。从图中可以看出,文中所提出的检测算法是主动式检测(Active Detection,AD),与被动式感应(Passive Response,PR)方法相比较,检测时间能缩短数十毫秒。

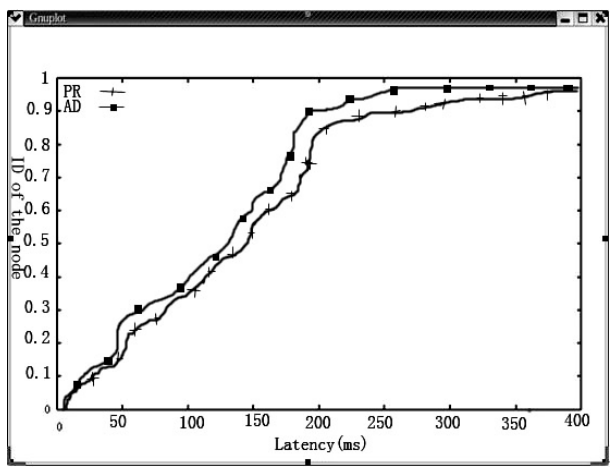

图 2 主动式检测与被动式感应方法的延迟比较

在信令开销方面,图 3 显示了不同修复策略中节点之间交互所需要的信令数量,它们的值都不超过 $\log n$,与理论结果一致。这一数值约是节点更改其 ID

的次数再乘以节点的度数。因此,从图 3 中也可以看出,度数增加越多的算法其信令开销就越大,意味着该算法的性能就越低,与前面的理论结果一致。

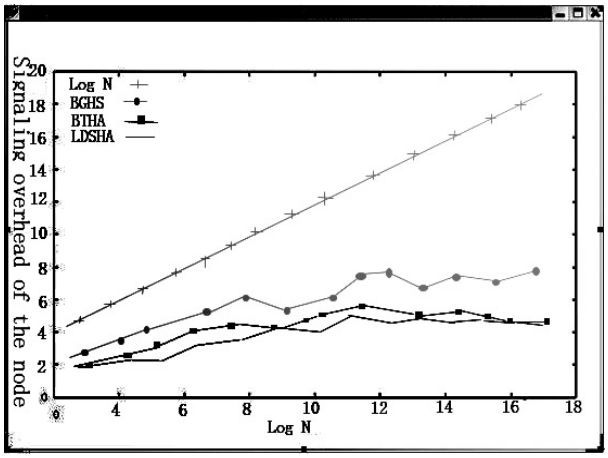

图 3　不同修复策略的信令开销

4　结束语

文中提出了一种在可重构网络中的自适应入侵检测修复算法,与其他算法相比,该算法不仅能够主动检测网络中的路径中断,还能够修复网络以保持连通性。经过实验,表明该算法不仅在检测延迟方面比传统的被动感应式方法少,而且在修复过程中节点度数增加的较少,节点之间的信令开销较小。

但是,该算法适用于某一特定时刻只有一个节点被删除,入侵者在删除下一个节点之前该算法已经将网络修复,如果入侵者同时删除多个节点,使多条路径中断,这种情况下的检测以及修复算法还需要进一步研究。

参考文献:

[1] 齐　宁,汪斌强,王志明. 可重构服务承载网容错构建算法研究[J]. 电子与信息学报,2012,34(2):468-473.

[2] 李　黎,管晓宏,蔡忠闽,等. 可重构网络系统的模型及体系结构[J]. 小型微型计算机系统,2009,30(4):637-641.

[3] 赵　靓,汪斌强,张　鹏. 可重构柔性网络体系研究[J]. 电信科学,2012,28(2):133-137.

[4] 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.

[5] Medard M, Finn S G, Barry R A. Redundant trees for preplanned recovery in arbitrary vertex-redundant or edge-redundant graphs[J]. IEEE/ACM transactions on networking, 1999,7(5):641-652.

[6] Andersen D, Balakrishnan H, Kaashoek F, et al. Resilient overlay networks[J]. SIGOPS oper syst rev,2001,35(5):131-145.

[7] 袁　博,汪斌强,孔维功,等. 可重构柔性网络中网络资源控制的冲突检测机制[EB/OL]. 2012. http://www.paper.edu.cn.

[8] Boman I, Saia J, Abdallah C T, et al. Self-healing algorithms for reconfigurable networks[J]. Lecture notes in computer science,2006,4280:563-565.

[9] Trehan A. Algorithms for self-healing networks[D]. USA: The University of New Mexico,2010.

[10] The Network Simultor-ns2[EB/OL]. 2011. http://www.isi.edu/nsnam/ns/.

[11] Yuan B, Wang B Q, Zhang B. A case study of green network-reconfigurable flexible network[J]. Telecommunication science,2011,27(10):200-208.

[12] Hitesh B, Paul F. CONMan: A step towards network manageability[C]//Proceedings of ACM SIGCOMM. Kyoto, Japan: [s. n.],2007:154-162.

(上接第 121 页)

test suites for interaction testing[C]//Proceedings of the international conference on software engineering. Portland, OR: [s. n.],2003:38-48.

[7] Kobayashi N, Tsuchiya T, Kikuno T. A new method for constructing pairwise covering designs for software testing[J]. Information processing letters,2002,81(2):85-91.

[8] Colbourn C J, Martirosyan S S, Mullen G L, et al. Products of mixed covering arrays of strength two[J]. Journal of combinatorial designs,2005,14(2):124-138.

[9] 于秀山,于洪敏. 软件测试新技术与实践[M]. 北京:电子工业出版社,2006.

[10] 严　俊,张　健. 组合测试:原理与方法[J]. 软件学报,2009,20(6):1393-1405.

[11] 王子元,聂长海,徐宝文,等. 相邻因素组合测试用例集的最优生成方法[J]. 计算机学报,2007,30(2):200-211.

[12] Kuhn D R, Wallace D R. Software fault interaction and implication for software testing[J]. IEEE transactions on software engineering,2004,30(6):1-4.

[13] 范明红,浦云明,汪志华. 等价类测试与划分研究[J]. 计算机技术与发展,2009,19(7):62-65.

可重构网络中自适应入侵检测修复算法研究

作者： 王超， 李永新， WANG Chao， LI Yong-xin

作者单位： 王超,WANG Chao(南阳理工学院 软件学院,河南 南阳,473004)， 李永新,LI Yong-xin(南阳农业职业学院 计算机系,河南 南阳,473061)

刊名： 计算机技术与发展

ISTIC

英文刊名： Computer Technology and Development

年，卷(期)： 2014(3)