doi:10.3969/j.issn.1001-893x.2013.10.015

舰艇实装网络多点评估数据实时采集*

刘喜作[1,2,**],王红军[2],毛建舟[2]

(1.大连理工大学,辽宁 大连 116024;2.大连舰艇学院,辽宁 大连 116018)

摘　要:为了提升舰艇实装模拟训练的反馈和评估功能,针对新型舰艇作战装备网络的特点,设计了在不同局域网里进行多点实时采集评估数据方法。该方法引入 WinPcap(Windows Packet Capture)工具,对网络适配器缓冲区的配置参数进行优化,实现了网络抓包性能的提升。同时,提出了通用数据解析机制,通过建立滑块模式缓冲区特有的读写方法,按照严密的解析流程对不断采集到的网络数据进行自动拆分、重组和舍弃方式来筛选查找,完成了对感兴趣评估数据的定点提取。实验结果表明,对于 100M 以太网,以 TCP 方式每秒传输小于 5 万个数据包(每个数据包长度为 228 字节),系统无丢包现象,并能对不同粘包进行正确还原,满足舰艇实装模拟训练对评估数据采集的需求。

关键词:舰艇实装模拟训练;WinPcap;数据采集;数据解析;训练评估

中图分类号:TN919;TP393　　**文献标志码**:A　　**文章编号**:1001-893X(2013)10-1331-05

Real-time Collection of Assessment Data from Multipoint in Actual Equipment Network of Warship

LIU Xi-zuo[1,2], WANG Hong-jun[2], MAO Jian-zhou[2]

(1. Dalian University of Technology, Dalian 116024, China; 2. Dalian Naval Academy, Dalian 116018, China)

Abstract: According to the characteristics of a new type of warship equipment network, the method of real-time collection of the assessment data from multipoint in different actual equipment networks is put forward to enhance the feedback and evaluation function of ship-borne simulation training. In this method, the toolkit of WinPcap(Windows packet capture) is used, and the data buffer parameter of the network adapter is optimized to enhance the performance of packet capture. At the same time, the general data analysis mechanism is proposed, and the special buffer block mode of reading and writing method is established. With the analytical process to implement the way of automatic separation, reorganization and abandon to filter and search the collected network data, it can position the interesting assessment data completely, correctly and real-timely. The experimental results show that the system can process up to 50 000 packets per second (each data packet length is 228 bytes) by TCP on 100M Ethernet link, so it satisfies the requirement of practical training in the warship simulation for assessment data collection.

Key words: ship-borne simulation training; WinPcap; date collection; date analysis; training evaluation

1 引　言

评估和反馈功能对于训练分析、成绩评定和经验总结具有重要意义,对提高受训者技能有极大帮助。而目前舰艇实装模拟训练的反馈和评估功能不够完善,在一定程度上制约了训练效果的提升[1]。利用舰艇作战系统现有的设备和网络资源,增加少量组件实现评估数据的实时采集将成为提高训练反馈的自动化和评估的智能化十分重要的环节。

在网络设备上实时侦听数据包进行分析是目前研究的一个热点。文献[2]指出,网络监测系统要考

* 收稿日期:2013-06-28;修回日期:2013-09-09　　Received date:2013-06-28;Revised date:2013-09-09

** 通讯作者:xizuoliu@163.com　　**Corresponding author**:xizuoliu@163.com

虑的性能因素有网卡驱动、过滤设置、数据包捕获时间戳、内存拷贝、系统调用、网络设备驱动中缓存的大小以及内核中数据包缓存的大小等。谢鲲[3]针对基于 WinPcap 的网络监控软件特点,给出了软件捕获的流量监测系统的总体性能评价。在解决高速网络环境中的丢包问题上,文献[4-5] 提出了基于 WinPcap 系统的性能优化方案,在分布式抓包结构方面进行了改进。而廖俊云[6]从抓包方法本身出发,提出了一种改进的快速抓包方法。但上述文献方法都没有提及如何对采集数据进行分析与筛选。

新型舰艇实装模拟训练网络在网络设备和通信协议与互联网有共性,但在网络架构和信息流程方面有独自特点。另外,评估数据实时采集系统更为关注对感兴趣的评估数据准确与完整提取。因此,本文针对这些特点,就舰艇实装模拟训练中评估数据实时采集方法进行论述。

2 实装模拟训练网络特点

开展实装化模拟训练,是以舰艇作战系统的整体性和系统性为基础,在构造的虚拟战场态势下进行的各系统(包括警戒探测系统、作战指控系统和软硬武器系统等)联合作战模拟训练,它需要各装备内部的局域网、作战指挥系统网和模拟训练外部网的共同支持。

2.1 训练信息流程

实装模拟训练是在实际舰艇装备上进行的作战训练。首先由嵌入式模拟训练设备或网络化模拟训练设备产生具有对抗性的训练态势,从警戒探测系统注入到实装上,为作战系统提供目标来源。警戒探测系统在不实际发射电磁波或声波的情况下模拟战场感知,进行战场信息获取。随后,将模拟获取的战场信息输入到作战系统内部,按照真实的作战信息流程在作战系统内部进行相应处理后,进行战场态势显示,使指挥员在如同实战的背景下进行目标识别、威胁判断、目标分配、火力打击等指挥决策。最后,各软硬武器系统收到目标指示,在指挥员下达火力打击命令后进行武器哑射、模拟攻击。整个训练过程与真实作战流程一致,既能训练指挥员的战术指挥能力,又能训练操作人员的装备操控能力[7-8]。

2.2 评估数据采集

评估系统要对上述整个过程进行跟踪,重点是对训练信息进行实时采集,主要包括考核目标的产生、发现、处理、上报、态势判别、目标指示和软硬武器攻击。而在训练过程中,训练信息要在不同的网络中流动,主要包括各警戒探测系统内部局域网、各软硬武器系统内部局域网、作战指挥系统网和模拟训练设备的内部网络等。另外,有的关键评估信息只在实际装备内部网络传输(如对考核目标的检测、攻击时机和方法等信息),设备间的通信又采用不同协议,这给训练评估信息采集增加了困难。

为了全面收集评估信息,完善舰艇实装模拟训练的反馈和评估功能,根据目前实际情况,评估数据采集设备必须进行多点数据采集。本文采用网络嗅探方法在不同网络上进行网络底层数据过滤与收集,采用通用解包机制进行评估数据分类解释,基本工作原理如图 1 所示。

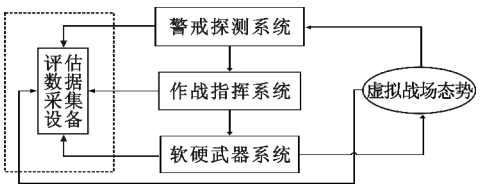

图 1 评估数据采集原理图

Fig. 1 The principle of assessment data acquisition

3 网络数据采集实现

评估数据采集的过程实际是对参与训练的各个网络流经信息进行监控与收集的过程,重点收集对考核目标实施作战行动的信息。为了全面准确地获得相应评估数据,系统采用了网络嗅探技术。

以单个网络的训练评估数据采集为例,我们采用以下几个主要的步骤:首先,打开网络适配器,配置相关参数控制接收数据的缓冲区和种类;然后,循环捕获数据包和采用通用解包机制分析处理数据包;最后,对得到评估数据进行记录,实现流程如图 2 所示。

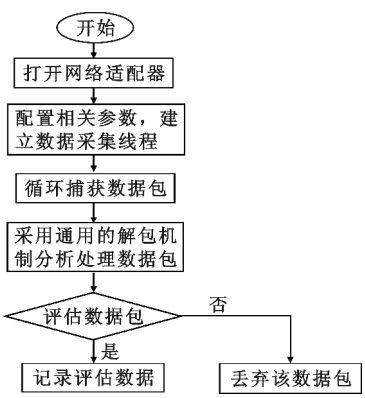

图 2 评估数据采集流程(单点)

Fig. 2 The process of assessment data acquisition(single point)

3.1　基于 WinPcap 网络数据获取

为了获得较好的移植性,本系统采用 WinPcap。WinPcap 提供了一个具有良好易用性和可扩展性的高效、通用且富于弹性的“内核”[9-10]。

WinPcap 一般抓包步骤有[11]:

(1)获取网卡设备列表(如果有多块网卡,则从中选择一块),设置用于嗅探的网卡和过滤器等参数;

(2)把网卡上的数据包复制到内核缓冲区中;

(3)通过上层的调用,把内核缓冲区中的数据包拷贝到用户缓冲区中,经过一定的处理,对采集的数据进行显示和保存。

3.2　配置相关参数

为了更加有效地对网络数据进行采集,必须认真配置 WinPcap 系统中的相关参数,主要包括网卡的设定、缓冲区的设定和数据过滤设定。

(1)网卡的设定

通过 pcap_open_live( ) 函数来进行网卡的设定。这个函数中共有 4 个参数,分别用来制定监听设备接口、制定 WinPcap 捕获的最大数目网络数据包、制定网卡工作模式和指定读数据的超时控制。其中关键是把网卡工作模式设置为混杂模式,当网卡处于混杂模式时它将接收所有的流经该网卡的数据包,这就意味着在共享介质的情况下可以捕获到其他主机的数据包。

(2)缓冲区的设定

WinPcap 的缓冲区包括内核缓冲区、用户缓冲区和内核缓冲区与用户缓冲区的拷贝数据最小值。系统的默认值分别为1 MB、256 KB和16 KB。为了提高抓包性能,在网络占用量大的情况下也能稳定工作,避免出现丢包的现象,可以适当提高上述值。

(3)数据过滤协议设定

根据所关心接收数据的特点,制定数据过滤协议方案,主要包括通信协议、网络端口、IP 地址和传输方向。在 WinPcap 中,捕获网络数据流和系统的捕获机制相集成,通过设置数据流过滤规则,在网络链路层实现对不需要数据直接过滤,而不需要拷贝到 WinPcap 的内核缓冲区内进行筛选,提高了效率。

3.3　数据采集线程

对于数据采集程序,可以用一个单独的线程进行数据采集。这样,能最大限度地保证采集的实时性,而另外的线程同时响应用户的操作和进行数据处理。

具体地说,基于 WinPcap 多线程数据采集需要完成以下工作:

(1)从 CWinThread 类派生一个自己的 PacketThread 类,这就是用于数据采集的类,进行采集时,创建一个 PacketThread 对象;

(2)数据采集线程的主体是一个 while 循环,为了简单直观,在该循环内包含了 WinPcap 的 pcap_next_ex( ) 方法,该函数反馈值大于零,表示有数据包到来,然后对数据包的基本信息进行解析,利用 SendMessage( ) 函数,通过事件的方式只把带有数据的报文传递给数据处理线程,而过滤掉如 TCP 中建立连接、关闭连接和连接重置等握手消息;

(3)工作结束,通过事件的方式关闭数据采集线程,利用 WinPcap 的 pcap_close( ) 函数,释放缓冲区,设置网卡为正常模式。

3.4　通用的数据解析机制

从数据采集线程得到的数据包汇集了实装局域网里进行传输的所有数据,而需要的评估数据是其中的一部分。我们建立了一个通用数据解析机制,对各种类型的数据包(TCP 包还是 UDP 包)和各种粘包现象(几个数据包粘结在一起或数据包接收不完整),都能有效地从这些数据中检测出和提取到感兴趣的评估数据。

(1)建立滑块模式缓冲区

建立一个缓冲区,缓冲区的大小一般是数据采集线程中内核缓冲区与用户缓冲区的拷贝数据最小值的几倍,以减少数据拷贝次数。该缓冲区的特点是通过有效数据开始滑块指针和有效数据结束滑块指针分别建立了有效数据区、过时数据区和空闲数据区,如图 3 所示。

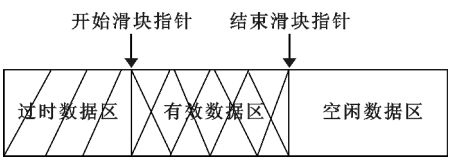

图 3　滑块模式缓冲区

Fig. 3 The slide buffer block mode

(2)滑块模式缓冲区写入方法

在写入时,如果准备写入数据的大小小于目前空闲数据区的大小,写入数据将直接拷贝到以现在结束滑块指针为起点空闲数据区内,同时结束滑块指针移动到刚刚写入数据的末端,形成新的有效数据区。如果准备写入数据的大小大于目前空闲数据区的大小,首先前移有效数据区覆盖掉过时数据区,使开始滑块指针重新回到缓冲区的起点,然后再进行写入数据的拷贝,拷贝结束移动结束滑块指针到刚刚写入数据的末端,形成新的有效数据区。

(3)滑块模式缓冲区读取方法

在读取时,只对有效数据区进行操作。如果要读取数据的大小小于有效数据区的大小,那么按该大小从有效数据区取走数据,同时开始滑块指针移动到刚刚取走数据的末端,产生新的有效数据区。如果要读取数据的大小大于有效数据区的大小,那么把有效数据区的所有数据取走,开始滑块指针将与结束滑块指针重合,使有效数据区的大小为零。

(4)数据包解释流程

评估数据包解释流程是指从有效数据区里查找出所需要的评估数据,取出并对其进行解释的过程。在数据处理线程中,对要接收的所有评估数据按网络传输的数据结构进行了定义,这些数据结构是由数据头和相应的数据内容组成,数据头中会规定类型和长度信息。在解释过程中可能出现 4 种情况:一是数据头长度不够;二是不是当前类的数据;三是数据长度不够;四是数据正确。解释时,用一个要查找的评估数据头在有效数据区开始滑块指针位置进行比较,如果有效数据区储存的数据大小小于评估数据头大小,返回数据头长度不够标识,等待滑块模式缓冲区继续写入数据;如果不是当前类数据,返回不是当前类的数据标识,进行下一个要查找的评估数据头的比较,如果这样查找下去,都不是需要的评估数据类头,将从有效数据区读取一个字节重新比较类型(这样可以滤掉不明的类型);如果判断是某个评估数据头但有效数据区大小小于该数据类型长度,表示接收不完整,返回数据长度不够标志,等待滑块模式缓冲区继续写入后续数据;如果是某个评估数据头并且有效数据区大小大于或等于该数据类型长度,返回数据正确标志,从有效数据区读取该评估数据即查找出所需要的评估数据,并继续上述解释过程进行查找。

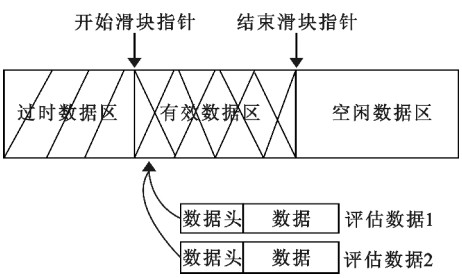

图 4 评估数据包解释

Fig. 4 Interpret assessment data

4 性能分析

在 CPU 为 1.0 GHz、内存为 2G、网卡为100M的两台计算机上,通过网线直接对接,进行性能分析,其中一台负责以 TCP 方式高速发送核心评估数据包(数据包长度为 228 B),另外一台负责评估数据包采集,同时把采集到的数据按上述通用解包机制进行自动还原。

性能测试时,设置 WinPcap 内核缓冲区、用户缓冲区和拷贝数据最小值分别为5 MB、2 560 KB和16 KB,定义滑块模式缓冲区为40 000 B。同一种情况测试180 s,然后取平均值。性能测试结果如表 1 所示。

表 1 性能测试结果

Table1 Performance test result

数据包/个	字节数/MB	抓包数	还原数	粘包率	丢包率
5 000	1.087	4 561	5 000	91.22%	0.00%
10 000	2.174	7 837	10 000	78.37%	0.00%
30 000	6.532	19 047	30 000	63.49%	0.00%
50 000	10.872	21 570	50 000	43.14%	0.00%
60 000	13.046	25 590	58 314	42.65%	2.81%
70 000	15.221	29 071	62 111	41.53%	11.27%

从表 1 可以看出,系统在高速网络下具有很低丢包率,但会出现大量的粘包现象。测试时,发送端发送固定 TCP 数据包,长度为228 B,而一次采集到的数据长度不等,试验中分别有228 B、1 460 B、136 B或456 B,表明几个数据包粘结在一起或数据包接收不完整。在没有丢包的情况下,即每秒传输小于 5 万个数据包,用通用解包机制都能自动准确还原;在有丢包的情况下,系统也会最大限度地准确还原数据。对于某新型舰艇实装模拟训练,模拟仿真系统的最大仿真度为 500 批目标,网络数据包每秒钟发送不会超过10 000个,流量不会超过2M,该方法完全可以胜任评估数据采集需求。

在每秒传输超过 6 万个数据包时,存在丢包现象。经分析,造成丢包的主要原因是由于用户缓冲区对数据包的处理方式过于复杂,当网络流量比较大时,用户缓冲区处理数据包的速度跟不上内核缓冲区从网卡复制数据的速度,所以新的数据包就会因为内核缓冲区满而被丢弃。进一步提高性能,需要对 WinPcap 内核拷贝过程进行优化,加快用户缓冲区处理数据包的速度。

5 总 结

本文论述了实装模拟训练网络特点,提出了在新型舰艇进行评估数据实时采集的方法,为了捕获流经各网络的所有数据,评估数据采集设备配置了多个网络适配器,分别接入舰艇各个系统相应网络

交换机的数据镜像口[12]。实践证明,该方法能完整、正确和实时地采集到感兴趣的评估数据,为基于实装模拟训练的网络数据自动化评估提供了有力技术支撑。另外,提出的通用数据解析机制也可以应用到舰艇串口通信方式的数据采集上,为下一步进行舰艇综合评估信息采集提供借鉴。

参考文献:

[1] 张锦荣. 推进海军模拟训练跨越式发展的几点思考[J]. 军事运筹与系统工程,2010,24(1):44-47.
ZHANG Jin-rong. Thought about Development of Sea Training Simulation[J]. Military Operations Research and Systems Engineering, 2010, 24(1): 44-47. (in Chinese)

[2] Loris D, Mario B, Fulivio R, et al. Profiling and Optimization of Software-based Network-analysis Applications [C]//Proceedings of the 15th IEEE SBAC-PAD. Sao Paulo:IEEE, 2003:226-234.

[3] 谢鲲,张大方,文吉刚,等. 基于 WinPcap 的实时网络监测系统[J]. 湖南大学学报(自然科学版),2006,33(2):118-121.
XIE Kun, ZHANG Da-fang, WEN Ji-gang, et al. A Real-Time Network Monitor System Based on WinPcap [J]. Journal of Hunan University (Natural Sciences), 2006,33(2):118-121. (in Chinese)

[4] 张伟,王韬,潘艳辉,等. 基于 WinPcap 的数据包捕获及应用[J]. 计算机工程与设计,2008,29(7):1649-1651.
ZHANG Wei, WANG Tao, PAN Yan-hui, et al. Data Packet Capture and Applications Based on WinPcap[J]. Computer Enginering and Design, 2008, 29(7): 1649-1651. (in Chinese)

[5] 吴鑫,余飞. 基于 WinPcap 的邮件信息解析系统的实现与优化[J]. 电子测量技术,2009,32(11):65-68.
WU Xin, YU Fei. Realize and Optimize of E-mail Information Analysis System Based on WinPcap[J]. Electronic Measurement Technology, 2009, 32(11): 65-68. (in Chinese)

[6] 廖俊云,范明钰,王光卫. 一种改进的基于 WinPcap 的快速抓包方法[J]. 计算机应用研究,2005,22(9):235-239.
LIAO Jun-yun, FAN Ming-yu, WANG Guang-wei. An Improved Fast-capturing Packet Method Based on WinPcap[J]. Application Research of Computers, 2005, 22(9): 235-239. (in Chinese)

[7] 徐军,陈大勇,周卫平,等. 舰艇作战系统嵌入式模拟训练技术研究[J]. 指挥控制与仿真,2008,30(6):110-113.
XU Jun, CHEN Da-yong, ZHOU Wei-ping, et al. Research on Embedded Simulation Training Technique for Naval Vessels Combating System[J]. Command Control & Simulation, 2008, 30(6):110-113. (in Chinese)

[8] 林平. 舰艇嵌入式模拟训练技术的应用及发展[J]. 军事运筹与系统工程,2008,22(4):28-31.
LIN Ping. Application and Development of Embedded Training Simulation Technology for Naval Vessels[J]. Military Operations Research and Systems Engineering, 2008, 22(4):28-31. (in Chinese)

[9] 沈辉,张龙. 基于 WinPcap 的网络数据监测及分析[J]. 计算机科学, 2012,39(10S): 15-18.
SHEN Hui, ZHANG Long. Network Data Monitoring and Analysis Based on WinPcap[J]. Computer Science, 2012,39(10S): 15-18. (in Chinese)

[10] 王月晖. 基于的网络数据捕获和分析系统的研究与实现[D]. 沈阳: 沈阳工业大学, 2007.
WANG Yue-hui. Research and Realize of Capture and Analyzation of Network Data Based on WinPcap[D]. Shenyang: Shenyang University of Technology, 2007. (in Chinese)

[11] 关朝辉. 多雷达系统数据包抓取与分析算法的设计[J]. 桂林航天工业高等专科学校学报,2011,61(1):7-9.
GUAN Chao-hui. Design of Data Packet Capture and Analysis Algorithm for Multi-Radar System[J]. Journal of Guilin College of Aerospace Technology, 2011, 61(1):7-9. (in Chinese)

[12] 马卉慧,董青,许都. 软交换中高速数据获取与过滤系统的设计[J]. 信息工程大学学报, 2010,11(5): 582-585.
MA Hui-hui,DONG Qing,XU Du. Design and Implementation of High-Speed Packet Capture and Filter System in Soft Switch System[J]. Journal of Information Engineering University,2010,11(5):582-585. (in Chinese)

作者简介:

刘喜作(1975—),男,辽宁庄河人,2004 年于海军大连舰艇学院获军事学硕士学位,现为讲师、博士研究生,主要研究方向为虚拟现实、作战仿真等;

LIU Xi-zuo was born in Zhuanghe, Liaoning Province, in 1975. He received the M. S. degree form Dalian Naval Academy in 2004. He is now a lectuer and currently working toward the Ph. D. degree. His research concerns virtual reality and combat simulation.

Email:xizuoliu@163.com

王红军(1962—),男, 山西高平人,2007 年于大连理工大学获工学博士学位,现为教授、博士生导师, 主要研究方向为电子对抗作战使用与仿真;

WANG Hong-jun was born in Gaoping, Shanxi Province, in 1962. He received the Ph. D. degree from Dalian University of Technology in 2007. He is now a professor and also the Ph. D. supervisor. His research concerns application and simulation of electronic warfare.

毛建舟(1975—),男,河南郑州人,2005 年于海军大连舰艇学院获军事学硕士学位,现为讲师、博士研究生,主要研究方向为作战指挥、作战系统等。

MAO Jian-zhou was born in Zhengzhou, Henan Province, in 1975. He received the M. S. degree from Dalian Naval Academy in 2005. He is now a lectuer and currently working toward the Ph. D. degree. His research concerns combat command and combat system.