4-2 A Load Balancing System for Mitigating DDoS Attacks Using Live Migration of Virtual Machines

ANDO Ruo, MIWA Shinsuke, KADOBAYASHI Youki, and SHINODA Yoichi

Recently, rapid advances of CPU processor make it possible to provide illusion that several operating systems is running at the same time, in multiplex way. Particularly, transferring virtualized OS technology called live migration, which moves virtual machine from one physical machine to another is promising technology for effective resource utilization and load balancing.

In this paper we propose a system for mitigating and protecting DoS (Denial of Service) attacks using live migration of virtual machine. In proposed system, we apply virtual machine monitor and modify the operating system which is virtualized. Then, we illustrate the detailed countermeasure for DoS attacks using live migration.

Keywords
Virtualization technology, Security, Denial of service attacks, Live migration, Load balancing

1 Introduction

Recent progress in CPU processor performance has allowed us to construct a virtual environment in which multiple operating systems (OS) run simultaneously. In particular, virtual machine monitors, which were used in the heyday of mainframe computers in the 1960s, have made a comeback in practical use with innovations in processor technology within the past few years. Virtual machine monitors are effective in streamlining resource utilization, load balancing, failure recovery, and reducing energy consumption. The present paper illustrates a strategy for mitigation of DoS (Denial of Service) attacks, which have come to pose a serious threat to current info-communication infrastructures, using virtual machine monitors. We then address the applicability of this strategy to defense systems.

2 Virtualization technology

Generally speaking, virtualization refers to a technology for establishing a many-to-one association between logical computer resources embodied in software and physical computer resources. Virtualization is analogous to the multiplexing process in electronic circuits, except that it is performed in the software layer. Advances in CPU processor performance within the last few years, especially the dramatic improvement in clock speeds, have enabled the provision of a virtual environment in which multiple OS are run simultaneously.

2.1 Classification based on architecture

Virtualization technology may be classified according to the layer in which virtualization is carried out. The major architectures of virtualization technology are as follows.

- Physical partitioning: The system is physically partitioned at the hardware level, and multiple OS are implemented. Although multiple OS may not be run simultaneously, failures and management of any one system will not affect the operation of other systems.
- Logical partitioning: Very similar to physical partitioning, except that the system is separated by partition monitors; as with physical partitioning, the OS are highly independent of each other.
- Virtual machine (OS): Performs hardware emulation on the OS level and carries out virtualization of the OS. CPU, memory units, devices, etc. are all virtualized on the OS level.
- Hosting: Resources such as CPU, memory units, devices, etc. are allocated to each application using the resource monitor. Low independence but high degree of aggregation.
- Virtual machine monitor: This is different from virtual machines in the sense that it exists intermediately between the hardware and the OS to reduce the overhead costs of virtual machines. The virtual machine monitor allows for changes in resource allocation, and its proximity to the hardware level permits it to have high independence.

Two factors in particular have contributed to the success of the virtual machine monitor: (1) the uniform management of device drivers by the host OS has facilitated the implementation and operation of the guest OS drivers; and (2) the provision of the complete virtualization of processor venders as a function of the virtual machine monitor has facilitated the implementation and operation of the virtual machine monitor.

The features offered for personal use by the virtual machine and the virtual machine monitor do not differ substantially. However, when the issue in question concerns loads and/or overhead costs of the server, etc., the virtual machine monitor will prove to be more effective.

2.2 Classification based on instruction set of processor

Virtualization technology may also be classified according to the instruction set of the processor. The processor may be subdivided into the application layer and the system layer. Virtualization in the application layer consists of multiprogramming, intermediate language operations, and binary translation. In the system layer, devices and OS are virtualized, as exemplified in the virtual machine and the virtual machine monitor.

Application level virtual machines

- Common instruction set: multiprogramming in which different resources are allocated to each application
- Dedicated instruction set: intermediate languages such as JAVA, binary translation, and user-mode QEMU

System-level virtual machines

- Common instruction set: virtual machine monitors such as VMWARE GX, XEN, and KVM
- Dedicated instruction set: the CPU is entirely virtualized to handle the different instruction sets. One example is the VIRTUAL PC, which emulates QEMU and MAC.

Presently, the technologies for increasingly advanced load balancing and debugging consist of those aimed at virtualizing common instruction sets on the system level.

2.3 Virtual machine monitor

The virtual machine monitor is situated intermediately between the hardware and the system level and provides virtualized hardware to the OS. It is usually possible to operate multiple systems on the virtual machine monitor. Dramatic progress in recent years has allowed for simultaneous operation of multiple OS in a virtualized environment. The virtual machine monitor’s intermediate position permits it to continue providing a robust operating environment in which a failure in one of the OS does not affect any of the other systems. Furthermore, with its direct emulation of hardware, resources allocated to each operating system may be dynamically changed.

3 Live migration

Live migration is a process in which a virtual machine in operation is transferred from one physical machine to another. To be more precise, the hardware is shared, and the memory state of one physical machine is sent to another machine. In a normal migration process, the state of the entire memory is first recorded prior to transfer, and thus the response to services provided by the virtual machine will be temporarily suspended. In contrast, in live migration, differential snapshots are transferred, allowing for a substantial reduction in the duration of service suspension during transferal.

4 Application for mitigation and prevention of DoS (Denial of Service) attacks

This section will introduce the effectiveness of transfer technology of virtual machines in the mitigation and prevention of DoS attacks. First, a method of transferring the system to provide the same service to a given address is used to counter attacks that exploit weaknesses in the system. Next, the method is used for load balancing as a measure to mitigate such attacks.

4.1 DoS attacks

DoS attacks are attempts to shut down the services of a targeted server by malevolent users (nodes), normally by over-consumption of bandwidth (network resources) and/or CPU and memory units (server resources), or by repeated attacks on a system vulnerability. DoS attacks have long been an issue in infocommunication security, and preventive measures have generally consisted of installation of load balancing devices (i.e., load balancers). The present paper proposes a system to prevent DoS attacks that utilizes the live migration process for virtual machine monitors. With the use of live migration, load balancing may be carried out at significantly higher granularity, and the proposed system has been proven to be particularly effective against DoS attacks that target system vulnerability.

4.2 DoS attack prevention measures

This section will describe the measures to mitigate and prevent DoS attacks using live migration. Figure 2 is a schematic diagram showing load balancing among multiple virtual machines for a service constructed on an

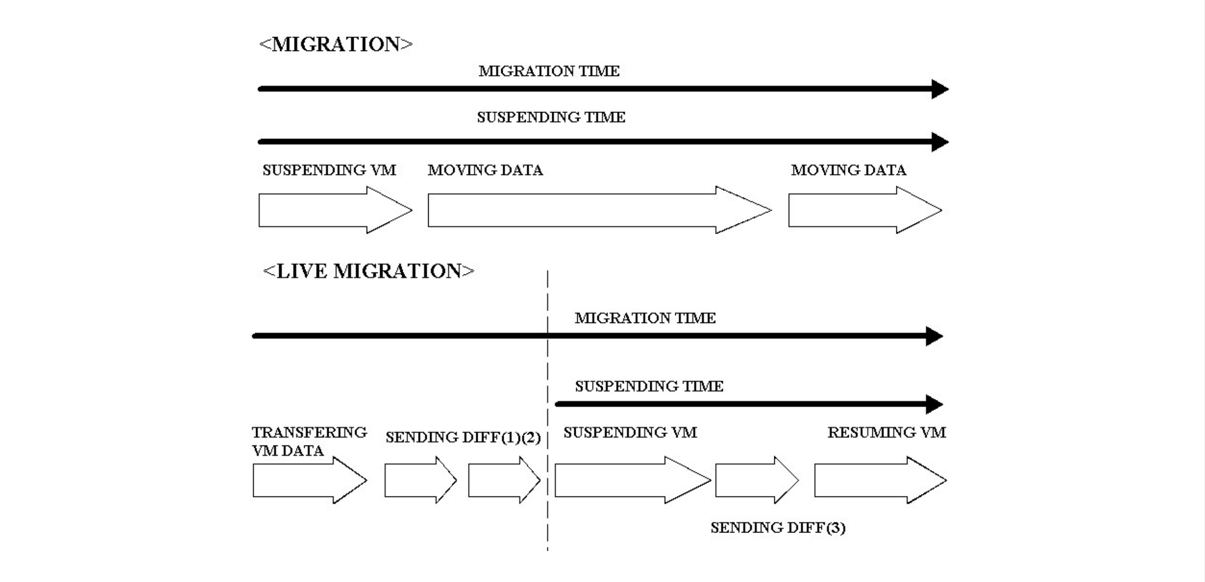

Fig.1 Live Migration

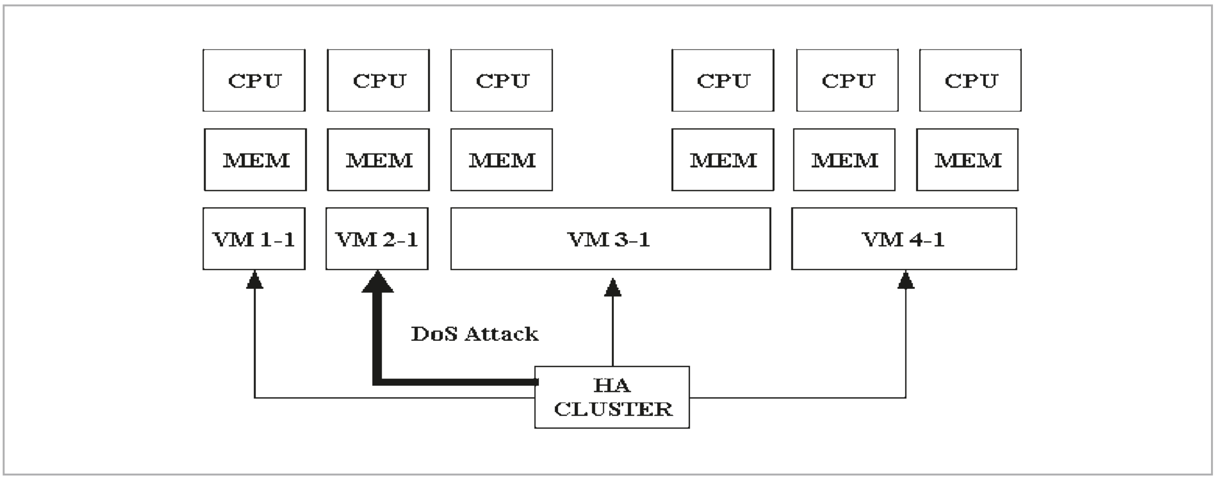

Fig.2 State of balancer prior to DoS attack

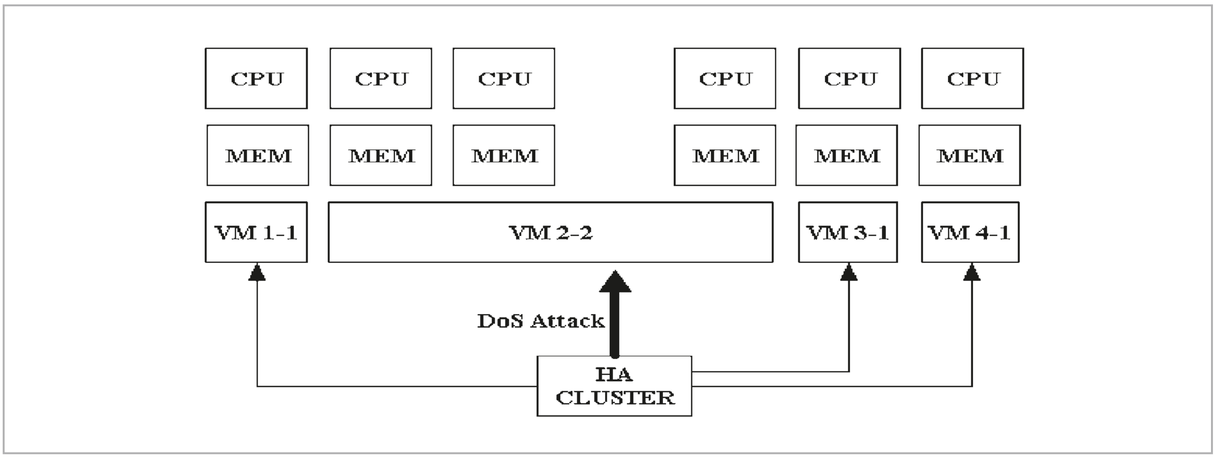

Fig.3 State of balancer after attack

HA (high availability) cluster. Here, it is assumed that VM1-1 and VM2-1 have fewer allocated resources compared to VM3-1 and VM4-1, and that DoS attacks are being made on VM2-1.

The prevention system in operation after attack is displayed in Fig. 3. Through live migration, more resources are allocated to VM2-2, which is under attack. This prevents the high load intentionally applied to VM2-2 from affecting mission-critical services and will mitigate the attack.

Furthermore, DoS attacks that target specific vulnerabilities in the system may be evaded by switching the version of the virtual machine. Application of the dynamic filtering rule may also be possible.

5 Conclusions

The recent dramatic advances in CPU processor performance have allowed for re-adoption of technologies for the virtual operation of multiple systems on a single physical machine, enabling the construction of a virtual environment in which multiple OS (operating systems) may be run simultaneously. In particular, virtual machine monitors, which were used in the heyday of mainframe computers in the 1960s, have made a comeback with the recent innovations in processor technology, and are now being implemented in practical applications. Among the noteworthy technologies is live migration, which dynamically transfers an OS in operation to another physical machine, and this method has been proven to be effective in streamlining resource utilization and load balancing.

The present paper introduced a method of designing measures to mitigate and prevent DoS (Denial of Service) attacks using the live migration of virtual machines. The system uses software forming a so-called virtual machine monitor in the detection of DoS attacks and for OS modification. Further, the paper presented an outline of the system to mitigate and prevent DDoS (Distributed Denial of Service) attacks using load balancing software (i.e., a load balancer) and live migration.

References

1 C. Clark, K. Fraser, S. Hand, J. G. Hansen, E. Jul, C. Limpach, I. Pratt, and A. Warfield, "Live Migration of Virtual Machines, In 2nd USENIX Symposium on Networked Systems", Design and Implementation (NSDI 05), p.273286, May 2005.

2 Ruo Ando, Youki Kadobayashi, and Yoichi Shinoda, "Incident-driven check pointer on full virtualized OS using KVM" IPSJ CSS (Computer Security Symposium) 2007, Nov. 2007.

3 Ruo Ando, Youki Kadobayashi, and Youichi Shinoda, "Incident-Driven Memory Snapshot for Full-Virtualized OS Using Interruptive Debugging Techniques", ISA 2008 The 2nd International Conference on Information Security and Assurance, Apr. 2008, Busan, Korea.

4 Ruo Ando, Youki Kadobayashi, and Youichi Shinoda, "Asynchronous nortification channel for exploitation-robust secure OS on virtual machine monitor", The 2nd Joint Workshop on Information Security, Aug. 2007, Tokyo, Japan.

5 Ruo Ando, Youki Kadobayashi, and Youichi Shinoda, "Asynchronous Pseudo Physical Memory Snapshot and Forensics on Paravirtualized VMM Using Split Kernel Module", ICISC 2007, The 10th International Conference on Information Security and Cryptology, Nov. 29-30, Seoul, Korea.

6 Nguyen Anh Quynh, Ruo Ando, and Yoshiyasu Takefuji, "Centralized Security Policy Support for Virtual Machine", USENIX, 20th Large Instllation System Administration Conference, Dec. 3-8, 2006 Washington, D.C.

7 Greg Goth, "Virtualization: Old Technology Offers Huge New Potential," IEEE Distributed Systems Online, Vol.8, No.2, 2007.

8 Paul A. Karger, Mary Ellen Zurko, Douglas W. Bonin, Andrew H. Mason, and Clifford E. Kahn, "A Retrospective on the VAX VMM Security Kernel", IEEE Trans. Software Eng. 17(11): pp.1147-1165, 1991.

9 Paul Barham, Boris Dragovic, Keir Fraser, Steven Hand, Tim Harris, Alex Ho, Rolf Neugebauer, Ian Pratt, and Andrew Warfield, "Xen and the art of virtualization", In Proceedings of the 19th Symposium on Operating System Principles(SOSP 2003), Bolton Landing, NY, Oct. 2003.

10 Tal Garfinkel and Mendel Rosenblum, "A Virtual Machine Introspection Based Architecture for Intrusion Detection", In the Internet Society's 2003, Symposium on Network and Distributed System Security (NDSS), pp.191-206, Feb. 2003.

11 Nguyen Anh Quynh, Ruo Ando, and Yoshiyasu Takefuji, "Centralized Security Policy Support for Virtual Machine", USENIX, 20th Large Installation System Administration Conference, Dec. 2006.

12 Uhlig, R, Neiger, G, Rodgers, D, Santoni, A. L, Martins, F. C. M, Anderson, A. V, Bennett, S. M, Kagi, A, Leung, F. H, and Smith, L, "Intel Virtualization Technology", IEEE Computer Vol.38, Issue 5, pp.48-56, May 2005.

ANDO Ruo, *Ph.D.*

Researcher, Traceable Secure Network Group, Information Security Research Center

Network Security, Software Security

MIWA Shinsuke, *Ph.D.*

Researcher, Traceable Secure Network Group, Information Security Research Center

Networks Security

KADOBAYASHI Youki, *Ph.D.*

Guest Expert Researcher, Traceable Secure Network Group, Information Security Research Center

Network Security

SHINODA Yoichi, *Dr. Eng.*

Executive Director of Information Security Research Center

Distributed and Parallel Computing, Networking Systems, Operating Systems, Information Environment