第33卷 第12期 计 算 机 工 程 2007年6月
Vol.33 No.12 Computer Engineering June 2007
·开发研究与设计技术· 文章编号：1000—3428(2007)12—0262—02 文献标识码：A 中图分类号：TP393

一种基于 Java 的安全 MANET 应用框架设计

陈东升，王培康
（中国科学技术大学电子工程与信息科学系，合肥 230027）

摘 要：无线自组织网络(MANET)中不同的终端设备和物理环境对网络行为有着非常大的影响。在对 MANET 的研究中，软件模拟并不能完全反映新协议在实际应用中的表现。开发现实中的测试平台和应用程序是促进 MANET 研究和发展必不可少的步骤。该文提出了一种基于 Java 平台的安全 MANET 应用框架——J-SMAF，在不影响网络应用的灵活性和扩展性的前提下，加入了对入侵侦测系统的支持，可以在不同的操作系统和应用环境下方便地构筑健壮、安全的 MANET 测试平台和应用系统。

关键词：无线自组织网络；Java；安全；入侵侦测系统

Design of Java-based Security MANET Application Framework

CHEN Dongsheng, WANG Peikang
(Dept. of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei 230027)

【Abstract】Mobile Ad Hoc networks (MANET) are highly dependant on the different types of nodes and the physical network environment. During the research on MANET, simulation can reflect only a partial behavior for the new protocols in the reallife. Deploying real-life MANET is therefore an indispensable complementary step for the advancement of MANET. This paper presents a Java-based secure MANET application framework——J-SMAF, which brings the intrusion detection system into the flexible and extensible application framework. With J-SMAF, people could build healthy and secure MANET real-life evaluation test-bed and application system easily on different platforms and in various environments.

【Key words】 Mobile Ad Hoc networks (MANET); Java; Security; Intrusion detection system (IDS)

1 概述

无线自组织网络(mobile Ad Hoc networks, MANET)是一种通过节点间的相互协作完成通信任务的新型网络。目前围绕着 MANET 领域路由协议、通信安全等重要问题已经有不少的探索和提案。然而，大多数的研究仍然停留在理论上，鲜有现实中实际应用的系统，这是因为首先各个方面的解决方案尚待有统一的标准；另外，多种多样的移动终端类型使得开发通用的 MANET 网络协议和应用框架也变得十分困难。

在实现的技术上，Java 语言以其跨平台的特性成为开发跨平台应用程序的首选。过去由于移动设备性能的限制和移动设备上 Java 虚拟机支持的不足，很少有基于 Java 语言的 MANET 应用尝试。近年来随着移动终端计算、存储能力的大大增强以及 Java 语言移动版本的拓展(MIDP2.0, CLDC1.1)，使得 Java 逐渐真正成为种类多样的移动、手持设备开发应用程序的利器。现在，已经有人提出使用 Java 语言开发 MANET框架的设想和模型，目前有FRANC[1]、SWANS[2]等。

FRANC 中将 MANET 框架分为协议栈、服务单元和消息池。其中在最核心的协议栈中将 MANET 作为虚拟网络构筑在 Java 语言提供的标准网络包之上，应用程序通过服务单元加入 MANET 虚拟网络，并由虚拟网络控制实际的网络节点进行通信。FRANC 提供了灵活的扩展接口，可以对现有的实现进行扩展，并通过配置文件对系统资源、协议栈进行配置。

SWANS 与 FRANC 不同，它在网络层和 MAC 层增加入了一个 Ad Hoc 层，使得用户可以直接使用常见通信协议如 TCP/IP 进行通信，而不需要了解 MANET 的接口。这样的设计实际上是将 MANET 的概念和实现进行了包装，使其对应用层透明。这无疑大大方便了新应用的开发和现有应用程序的移植。

然而，FRANC和SWANS在扩展性上的考虑都只是出于对异构网络和新路由协议的适应，它们忽略了网络中另一个非常重要的方面：安全。虽然在FRANC和SWANS中可以通过采用安全性更强的路由协议来增加恶意节点和程序破坏MANET的难度，但事实证明入侵者总能找到网络的漏洞。尤其是MANET这类开放信道、移动性强的网络，更容易受到攻击。健康、完整的MANET网络体系需要有安全性强的在网络受到入侵时能找到异常节点的能力，并作出反应，以防止更大的破坏。这就是入侵侦测系统(intrusion detection system, IDS)[3,4]。在现有的几种基于Java平台的MANET应用框架上都无法灵活地实现入侵侦测系统，也就是不能构筑完整的MANET安全体系。

本文提出了一种基于 Java 平台的安全 MANET 应用框架——J-SMAF(Java-based Secure MANET Application Framework)。

2 J-SMAF 设计

J-SMAF 的核心由两部分相对独立的框架组成：基础网络框架和基于日志的 IDS 框架。基础网络框架提供支持 MANET 通信的协议栈和应用程序接口，并通过事件日志的方式为 IDS 的实现提供支持。IDS 框架借鉴文献[2,3]中的思想，设计了基于本地代理和移动代理的分布式入侵侦测系统

作者简介：陈东升(1981－)，男，硕士生，主研方向：计算机网络；王培康，教授

收稿日期：2006-07-06 **E-mail：**cdschen@mail.ustc.edu.cn

实现接口。两方面可以独立地实现和配置，满足不同的应用和安全需要。

2.1 基本网络框架

基本框架是一组构筑在移动的终端操作系统和 Java 虚拟机之上的网络协议接口和应用程序，为各种不同的终端上的应用提供了 Ad Hoc 模式通信的支持。在网络通信协议栈接口的设计上借鉴了 SWANS 的特点，将 Ad Hoc 层置于较底层的位置，以简化最终应用程序的开发和移植。与其他框架不同的是，通过一个特殊的日志重写器对协议各层接口的实现类进行动态的重写，统一地记录各层面的事件日志，通过事件日志的形式提供对入侵侦测系统的支持。如图 1 中灰色区域所示。

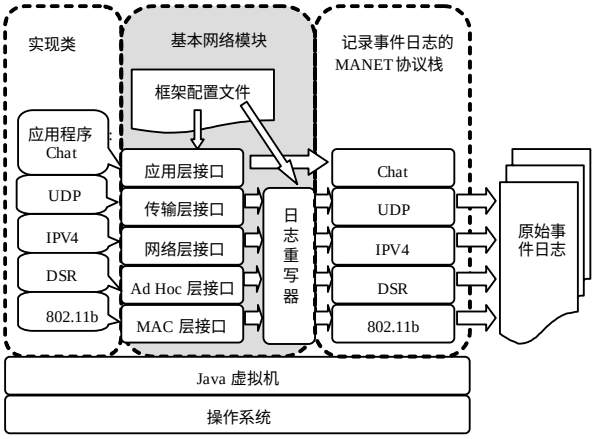

图 1 J-SMAF 的基本网络框架

基本网络框架由以下部分组成：

(1)应用层－MAC 层接口 :定义了 MANET 协议栈各个层面的不同协议需要实现的接口，每个层面为其相邻层面提供相应的调用函数。

(2)日志重写器：基于传输层到 MAC 层的各接口定义的方法，对这些接口具体的实现类进行重写，使重写后的实现类具有记录网络事件、生成事件日志的能力。

(3)框架配置文件：配置日志重写器、各层接口。通过框架配置文件可以在实际应用中根据对环境、性能和安全等方面的不同需求灵活地对框架进行配置。

在图 1 中，实现类区域内是实现各层协议接口的普通 Java 类，它们实现了整个应用框架各层协议的基本功能。基本网络框架通过框架配置文件将它们加载以后，日志重写器依据协议栈定义的接口对相应的实现类进行重写。重写后的类会在运行时记录接口定义的方法的执行日志，生成原始事件日志。这些经过重写的实现类组成了实际运行的 J-SMAF 网络协议栈。

2.2 IDS 框架

以基本网络框架生成的原始事件日志为基础，J-SMAF 的 IDS 框架的构成组件如图 2 所示，由以下 6 部分组成：

(1)日志分析器：将原始事件日志分类，处理，转换成便于 IDS 分析处理的形式，即抽象事件日志。

(2)代理控制器：控制加载或删除本地、异地安全代理。代理控制器可以同时加载多个不同的本地代理或异地代理实现类。本地代理和异地代理之间的通信也由代理控制器进行。

(3)本地代理接口：定义了驻留在本地的安全代理模块。它的实现类通过代理控制器对抽象事件日志进行访问，不同的实现类使用各自的逻辑对抽象事件日志进行分析，用于侦测不同种类的入侵。

(4)异地代理接口：定义了来自其它节点的代理模块。异地代理属于移动代理的一种，可以根据需要发送到其它节点上执行，收集保存在其它节点上的需要的信息与本地代理联合分析侦测可能的入侵行为。

(5)代理通信接口：定义了本地代理和异地代理之间进行通信的接口，具体的实现可以借助基本网络框架，也可以是专门实现的安全通道。

(6)IDS 配置文件：配置日志分析器、抽象日志、代理控制器。通过 IDS 配置文件可以灵活地控制 IDS 加载的各个组件和安全警报级别。

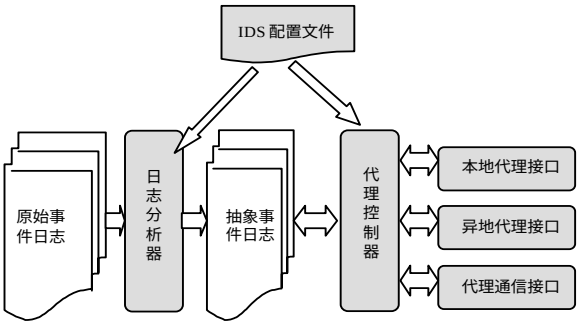

图 2 J-SMAF 的 IDS 框架

在 J-SMAF 的 IDS 框架中固定的组件是日志分析器和代理控制器。根据 IDS 配置文件的不同配置，日志分析器对原始事件日志生成相应粒度的抽象事件日志，代理控制器加载相应的本地安全代理逻辑并控制异地代理的执行权限。

J-SMAF 的 IDS 框架中实际执行入侵侦测逻辑的是本地代理和异地代理，它们实现了框架定义的基本功能接口，每种代理实现对一种或几种入侵行为的侦测。它们可以通过配置文件进行灵活的加载和卸载。整个 IDS 可以侦测的入侵行为也可以通过实现新的安全代理进行扩展。

3 安全讨论

J-SMAF 中 IDS 框架工作的基础是事件日志。与普通日志的记录形式不同，面向基本网络框架协议栈中定义的接口，利用 Java 语言的特点使用日志重写器来重写协议栈的实现类，使其具有记录事件日志的能力。这样做一方面使开发者在实现各层接口时只需要关注协议核心算法的实现，而不必考虑网络其它方面的需求，减少了系统模块之间的耦合；另一方面，系统对日志重写器进行封装，仅开放协议栈的接口和配置文件，杜绝了恶意节点通过不记录日志或伪造日志来躲避入侵侦测系统的企图。

J-SMAF 通过事件日志的形式使基本网络框架和 IDS 框架有机地结合起来，同时又可以对二者进行独立的实现和配置，在网络协议和安全保障手段上都提供了充分的灵活性和扩展性，在安全需求较低的环境中，用户可以在基础网络框架上配置效率更高的路由协议，记录较大粒度的事件日志；在 IDS 框架上配置最基本的安全代理来侦测最常见的入侵，甚至关闭 IDS，从而节省系统资源、提高系统效率。反之，在安全需求较高的环境中，用户可以通过配置文件在基础网络框架上使用安全性更强的路由协议，记录最细粒度的事件日志；在 IDS 框架中加载全部的安全代理以及更高的报警级别来保障系统安全。

4 总结

在完整、健壮的 MANET 体系中，入侵侦测系统是必不可少的部分。本文提出的 J-SMAF 框架综合了文献[1]灵活的扩展性和文献[2]便于应用程序开发和移植的特性，并且引入了事件日志机制和基于事件日志的入侵侦测系统。基于 J-SMAF 框架，开发者可以根据使用环境的不同，灵活地开发和配置健壮、安全的 MANET 应用系统。 (下转第 266 页)