第 35 卷 第 3 期 计 算 机 工 程 2009 年 2 月
Vol.35 No.3 Computer Engineering February 2009
·安全技术· 文章编号：1000—3428(2009)03—0192—03 文献标识码：A 中图分类号：TP393.08

基于代理的分级 MANET 入侵检测系统

姚越鹏，钟求喜
(国防科技大学计算机学院，长沙 410073)

摘 要：针对分级移动自组织网络(MANET)中的安全检测问题，拓展分布式协作 IDS，提出一种基于代理的分级 MANET 入侵检测系统。该系统采用分簇检测和簇间联合检测的方法，为分级 MANET 防护提供一种新的入侵检测方案。实例分析和实验仿真结果证明，该检测系统有效。

关键词：分级 MANET；入侵检测系统；入侵检测代理

Agent-based Intrusion Detection System for Classified MANET

YAO Yue-peng, ZHONG Qiu-xi
(School of Computer Science, National University of Defense Technology, Changsha 410073)

【Abstract】 Aiming at the security of agent-based distributed cooperative intrusion detection framework that suits hierarchical Mobile Ad Hoc Networks(MANET), this paper extends the distribute cooperation IDS, puts forward an agent-based intrusion detection system for classified MANET. The system adopts cooperation detection method of clusters, and provides further intrusion detection scenario for protecting hierarchical MANET. Detailed analysis and simulations are carried to validate the effectiveness of our detection model for attacks.

【Key words】 hierarchical MANET; intrusion detection system; intrusion detection agent

1 概述

由于对系统的攻击难以避免，因此有必要在移动自组网(Mobile Ad-hoc network, MANET)中部署入侵检测系统(Intrusion Detection System, IDS)来监控系统状态。在分级结构 MANET 中，网络被划分为多个网络簇，簇头节点位于所在区域的中心位置，负责网络中组织和管理的工作。簇头节点形成高一级骨干网络，通过再次划分网络簇可向上扩展网络层次。在实际应用中，当 MANET 网络规模较大时，分级网络结构具有更高的安全性和实用性。

基于以下假设：(1)不考虑何种代理节点，假设已有较好的代理分发算法；(2)不考虑簇头选择和簇形成算法。(3)不考虑节点自私性。本文在分布式协作 IDS 的基础上，以簇为基本单元，以簇头为主要节点，设计基于代理 IDS 体系结构和 Agent 结构的分级 MANET 入侵检测系统(C-MANET-IDS)，并针对不同级别的节点分析入侵检测和响应的过程。

2 系统体系结构设计

文献[1]提出一种适用于 MANET 的分布式协作 IDS，为本文的分级 MANET 的入侵检测系统设计工作奠定了基础，文献[2-3]也为本文的研究提供了突破口。在分布式协作 IDS 中，每个节点都参与入侵检测与响应，通过 IDS 代理收集本地信息独立地进行本地入侵的检测，通过联合检测获得更大范围的检测数据进一步确认是否遭受攻击。检测代理主要包括 6 个功能模块：数据收集，本地检测，合作检测，本地响应入侵，全局入侵响应和安全通信。该入侵检测方案符合 MANET 分布式网络结构的特点，并在一定程度上扩大了收集数据和检测的范围。但将它直接应用于分级 MANET 还存在一些问题：(1)不适合分级 MANET 的体系结构，不能根据节点能力的不同分配不同的任务。(2)没有考虑能源问题，不是所有节点都可以承受相同的代理模块。(3)要获得更优的性能与效果，应考虑分级 MANET 区别于平面结构 MANET 的网络特性。

设计 IDS 体系结构也应遵循与系统本身的体系结构相适应的原则。考虑分级 MANET 区别于平面结构 MANET 的特点：(1)层次体系结构；(2)簇头节点可获得一定程度的互联；(3)簇头节点具有较强的能力；(4)能力有限的簇内成员节点以簇头节点为核心形成网络簇；(5)采取较平面结构严格的信任模型。C-MANET-IDS 的体系结构如图 1 所示。

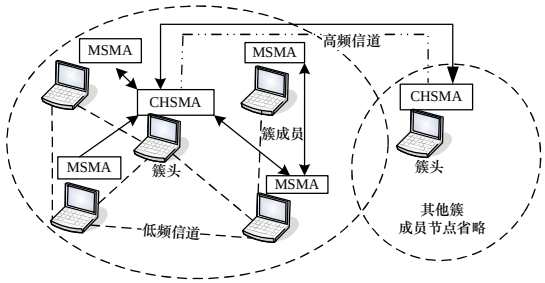

图 1 C-MANET-IDS 体系结构

其设计思想包括以下几点：

(1)簇作为基本检测单元，在簇内收集检测数据，入侵检测尽量在本簇内完成。

(2)簇头节点和簇内成员节点分别使用不同的 IDS 代理，其中 CHSMA 是簇头代理，MSMA 是簇内成员代理。

作者简介：姚越鹏(1979－)，女，硕士，主研方向：分级 MANET 的安全防护体系，分级 MANET 的入侵检测系统；钟求喜，副研究员、博士

收稿日期：2008-06-12 **E-mail：**glassgirl@yeah.net

(3)簇头节点作为汇总数据、分析数据、确定入侵的检测节点。

(4)簇内成员节点的主要工作是收集数据。

(5)簇头节点将入侵向 2 级节点广播，将入侵节点在全网内列入黑名单。

(6)出现可疑入侵时，由簇头节点向其他簇头节点发起联合检测的请求。

在分级 MANET 的网络结构中，将 IDS 的主要工作交给簇头节点较为合适。IDS 需要大量的通信开销，并且要求尽量获得全局信息，而簇头节点的计算能力和通信能力较强，连通性也更为可靠。而簇内成员节点计算能力与通信能力较弱，如果赋予太多 IDS 的责任，会严重影响到网络正常的工作。

IDS 要完成检测任务，应尽量掌握到全局信息，因此，需要簇内成员节点的配合，即采用代理技术(软件代理模块或专用代理节点)来随机采样数据，簇内成员节点只需进行数据收集的工作。

3 系统代理结构设计

如图 2 所示，C-MANET-IDS 系统的代理结构包括簇头代理模块(Cluster Head Secure Manage Agent, CHSMA)和簇内成员代理模块(Member Secure Manage Agent, MSMA)。

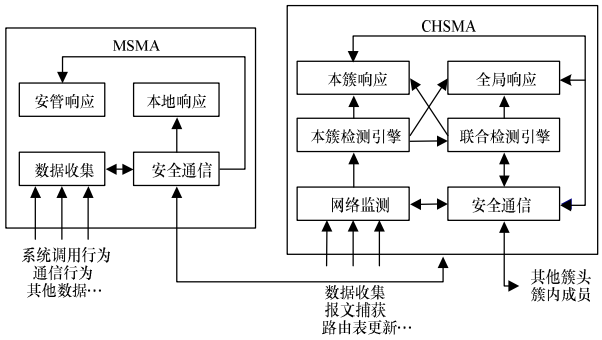

图 2 C-MANET-IDS 的代理模块结构

各模块功能如下:

(1)CHSMA

网络监测: 接收各成员节点传送的数据，监测网络数据，如捕获报文，监控路由表的更新等，对收集的数据进行分类、计算等处理。

本簇检测引擎: 分析数据，确认是否被入侵，在必要时触发联合检测请求。

联合检测引擎: 当本簇检测引擎不能确认入侵时，就会触发联合检测请求，请求其他簇联合检测。触发规则是触发与本簇可能入侵节点在某时间段内有通信的簇。联合检测过程为: 1)发送联合检测请求，并传递本簇内检测状态信息报告，指出可能的入侵或异常。2)其他簇头判断本簇是否收到报告中指出的可能入侵和异常报文。3)其他簇头根据自己簇内的数据做出判断，给出攻击的可能百分比。4)根据其他簇与可疑节点的通信量和给出的攻击百分比，发起请求的簇头使用加权平均算法，遵循少数赞成多数的原则，确认是否入侵或异常。

本簇响应: 决定响应策略，在簇内广播，并在 2 级节点之间广播。可能的响应策略有重新初始化认证信息，重新初始化信道，黑名单操作等。

全局响应: 一般是黑单名单操作，即在全网隔离某个入侵节点。

(2)MSMA

数据收集: 由多个数据收集模块组成，主要收集有用的数据流。包括节点内部的系统和用户行为、节点传播范围内的通信行为以及与安管相关的一些设备、能源使用情况等。

本地响应: 簇头确认入侵或攻击后，通过本簇响应模块决定相应的响应策略，并通过安全通信模块向本簇内节点下发策略。因此，MSMA 中的本地响应模块主要用于处理响应策略。如重新初始化本簇的分布式认证密钥，修改路由表等。

(3)安全通信

CHSMA 和 MSMA 都包括一个安全通信模块，主要为节点之间提供高信任的安全通道，并且能格式化 IDS 数据，以获得更高效的分类、分析和处理。

(4)簇头间的信任模型

主要针对黑洞攻击建立簇头间的信任模型，即监测报文转发的情况: 1)簇头间通过网络监测模块和不可否认机制建立信任模型。2)域间转发时，源簇头监视目的簇头是否转发报文。3)无法确定攻击时，采取投票机制确定是否目的簇头已经被占领。4)一旦认定目的簇头是恶意节点，则孤立该簇。

(5)CHSMA 入侵检测流程

CHSMA 的入侵检测流程如图 3 所示，监测模块通过 MSMA 收集本簇内的数据，并监控各成员节点的网络行为，由本簇检测引擎进行数据分析和处理，一旦发现入侵则在全网响应，如不能确认入侵则发起联合检测请求，由相关簇头投票来决定入侵。

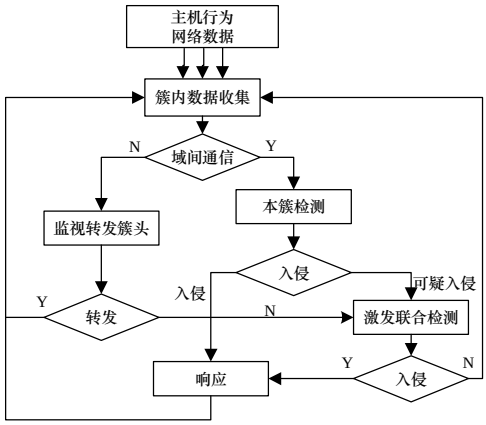

图 3 CHSMA 入侵检测流程

4 实例分析

本文针对 C-MANET-IDS 不同级的恶意节点，分别讨论攻击过程中的检测与响应过程。在分级 MANET 网络中，簇头节点可通过高频信道互联。簇头节点驻留在 CHSMA 模块中，成员节点驻留在 MSMA 模块中。其中，MSMA 负责收集数据，CHSMA 则通过汇总 MSMA 收集的数据监视簇内成员节点行为。

4.1 恶意节点为簇内成员节点的情况

以 AODV 攻击为例，如图 4 所示，A_1 开始发起拒绝服务攻击，向簇内发送大量 RREQ 路由查询报文，报文在网络中扩散，占用和消耗大量网络资源，降低了网络的服务性能。

(1)A_1 请求到达不存在节点的路由

当 A_1 发出这样的 RREQ 报文时，A-CHSMA 的网络监测模块将该条报文消息记录在报文信息表中，匹配 IP 地址表后，发现并不存在该地址的节点，A-CHSMA 会向其他簇

CHSMA 请求检测该 IP 地址，如无法匹配，则认为 A_1 发起伪造 IP 攻击，从而在全网进行入侵响应。

(2)A_1 请求到达簇内节点的路由

当 A_1 发出这样的 RREQ 报文时，路由查询报文只会在簇内扩散。首条不同目的地址的 RREQ 报文可能会被处理，一旦该节点所发送的 RREQ 报文超过阈值，则 A-CHSMA 认为 A_1 发起泛洪攻击，从而全网进行入侵响应。

(3)A_1 请求到达其他簇节点的路由

当 A_1 发出这样的 RREQ 报文时，例如，请求到达 B_3 的路由，路由查询报文会在全网内扩散，其危害最大。A_1 发送的首条不同目的地址的 RREQ 报文仍可能被处理，与 2 相同，超过阈值后，A-CHSMA 会认为 A_1 发起泛洪攻击，从而在全网内响应。在这个过程中，可能由于 A_1 在某时间段内发出的路由查询报文未超过阈值而没有被 A-CHSMA 发现攻击，但由 A_1 发出的 RREQ 报文可能在其他簇内转发，例如 *B* 簇，那么 B-CHSMA 监测到这一情况就会向 A-CHSMA 发起联合检测请求，如果仍不能确定攻击就会向网内其他 CHSMA 发出联合检测请求，投票决定 *A*1 是否为恶意节点，一旦认为 A_1 为恶意节点，则在全网内响应。

(4)响应过程

一旦确定 A_1 为恶意节点，则 A-CHSMA 首先在簇内发起入侵响应，对节点 A_1 进行隔和黑名单操作。同时，A-CHSMA 在簇间发起入侵响应，使 A_1 节点无法通过重新认证回到网络。

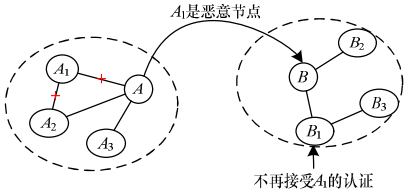

图 4　响应恶意成员节点

4.2　恶意节点为簇头的情况

以 AODV 路由协议为例(图 5)，*B* 发起黑洞攻击，对收到的报文不转发而是全部丢弃，从而影响网络的正常工作。

(1)检测过程

域 I 中的节点 *a* 与域 II 中的节点 *b* 需要通信，*a* 将报文发给簇头节点 *A* 要求转发，簇头 *A* 将报文转发给簇头 *B* 后 A-CHSMA 就开始监测 *B* 的网络行为。*B* 收到域间转发的报文回复一条签名的确认消息给 *A*，A-CHSMA 如果在预定的时间段内发现 *B* 没有转发报文则向其他簇 CHSMA 发出联合检测请求，并将 *B* 回复的确认消息作为通信状态信息之一发送给其他簇头节点。其他簇头通过查询历史状态，或通过测试进行投票，一旦确认 *B* 已经是恶意节点，则进行全网响应。如果认为 *B* 不是恶意节点，则 *A* 将再次发送须转发的报文，重新开始新一轮的监视，这样，如果 *B* 多次无法转发报文，则被确定为攻击节点，或 *A* 将选择其他路由转发。

(2)响应过程

一旦确定 *B* 为恶意节点，则 A-CHSMA 在簇间发起入侵响应，使 *B* 簇被隔离，但只有 *B* 节点被执行黑名单操作，II 内的成员节点可能在一段时间无法通信后离开 II，然后通过重新认证加入其他簇从而回到网络中。

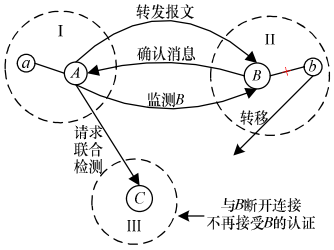

图 5　检测和响应恶意簇头

5　结束语

本文通过探讨分布式协作入侵检测框架，设计基于 Agent 的分级 MANET 入侵检测系统的体系结构和 Agent 结构。该检测系统通过遍布整个网络的 Agent 对报文进行监测，采用 MSMA 与 CHSMA 交互机制，分离数据收集和监控的功能，降低网络节点的消耗，可减轻成员节点的负担，并能对网络中同时存在的多处入侵活动作出反应。实例分析和实验仿真结果表明，该系统的检测率能达到 80%以上，虽然占用了部分网络开销，但能改善攻击情况下的网络性能，有 IDS 的 MANET 在攻击下的网络性能维持在 70%左右，证明了该检测系统的有效性。

参考文献

[1] Zhang Yongguang, Lee W. Intrusion Detection in Wireless Ad-Hoc Networks[C]//Proc. of MOBICOM '00. Bostan, MA, USA: [s. n.], 2000: 275-283.

[2] Karygiannis A, Antonakakis E, Apostolopoulos A. Detecting Critical Nodes for MANET Intrusion Detection System[C]//Proc. of the 2nd International Workshop on Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing. Lyon, France: IEEE Computer Society Press, 2006: 7-15.

[3] Srinivasan T, Vijaykumar V, Chandrasekar R. An Auction Based Task Allocation Scheme for Power-aware Intrusion Detection in Wireless Ad-Hoc Networks[C]//Proc. of IFIP International Conference on WOCN'06. Bangalore, India: [s. n.], 2006: 1-5.

（上接第 138 页）

[4] Wang Hui, Osada S, Yokohira T, et al. Throughput Optimization for TCP with an Active Proxy in Long-delay Satellite Environments[C]//Proc. of 2006 Joint Conference on Satellite Communications. Osaka, Japan: [s. n.], 2006: 125-130.

[5] Osada S, Wang Hui, Yokohira T, et al. Throughput Optimization in TCP with a Performance Enhancing Proxy[C]//Proc. of International Conference on Communication Technology. Guilin, China: IEEE Computer Press, 2006: 392-397.

[6] Wang Hui, Osada S, Yokohira T, et al. Effect of Premature ACK Transmission Timing on Throughput in TCP with a Performance Enhancing Proxy[J]. IEICE Transactions on Communications, 2007, 90(1): 31-41.

[7] Floyd S, Henderson T, Gurtov A. The NewReno Modification to TCP's Fast Recovery Algorithm[S]. RFC 3782, 2004.

[8] Blanton E, Allman M, Fall K, et al. A Conservative Selective Acknowledgment(SACK)-based Loss Recovery Algorithm for TCP[S]. RFC 3517, 2003.