第 33 卷　第 19 期　　计　算　机　工　程　　2007 年 10 月
Vol.33　No.19　　Computer Engineering　　October 2007
·博士论文·　　文章编号：1000—3428(2007)19—0013—03　　文献标识码：A　　中图分类号：TP393

MANET 分簇 IDS 告警消息保全传递的一种方案

李胜广，刘建伟，张其善
（北京航空航天大学电子信息工程学院，北京 100083）

摘　要：介绍了移动Ad Hoc网络中入侵检测系统的结构，分析了一种加权分层IDS系统和分簇算法。根据这种分层结构，阐述了一种利用数字签名传递与广播告警信息的一种方案。设计了自组网中入侵检测告警信息的包数据格式，给出了ELFhash哈希函数的实现代码。
关键词：移动 Ad Hoc 网络；入侵检测系统；加权选簇；哈希函数

Scheme of Alert Message Integral Transferring for Clustering IDS in MANET

LI Sheng-guang, LIU Jian-wei, ZHANG Qi-shan
（School of Electronic and Information Engineering, Beijing University of Aeronautics and Astronautics, Beijing 100083）

【Abstract】This paper introduces the structure of intrusion detection system in mobile Ad Hoc networks, and analyzes a model of layered weighted IDS and clustering algorithm. According to the hierarchical structure, it gives a scheme of broadcasting and transferring alert message using digital signature. It designs the packet format of alert message, and gives the source code of ELFhash Hashing function.
【Key words】mobile Ad Hoc networks(MANET); intrusion detection system(IDS); layered weighted clustering; Hashing function

移动Ad Hoc网络(mobile Ad Hoc networks, MANET)是一种不依赖于任何预先定义的基础架构，由一组带有无线收发装置的移动终端组成的多跳临时性自组织网络[1]。MANET面临的一个主要挑战就是容易受到安全攻击，比如受到窃听、伪造、拒绝服务等攻击。虽然加密、认证等安全技术的应用可以有效地减少MANET的入侵，但是不能彻底地消灭入　侵[2]。入侵检测系统(intrusion detection system, IDS)则成了安全防范的第 2 道防线。一旦入侵行为被检测到，整个网络就能够及时产生反应，保证网络的安全以减少损失。

MANET 中节点分散，IDS 中的告警信息没有统一的日志服务器集中管理，告警信息成为相互节点之间提醒和警告的载体。但是 IDS 之间的告警信息传递是不安全的，如何将已经检测到的入侵事件及时正确地广播出去是非常关键的，就像战场上的侦察员侦察到敌情，需要立即送到其组织，不然侦察行为毫无意义。本文就 MANET 这种特殊的网络拓扑下分层的 IDS 如何完整地传递告警信息进行分析，并给出了自己的方法。

1　加权分簇 IDS 模型

MANET 网络结构通常分为平面结构和分层结构。MANET 中的 IDS 系统按结构层次也分为平面结构和分层结构。平面结构的 IDS 中每个节点或者部分节点利用本地检测模块参与入侵检测过程。当本地检测模块发现入侵行为就广播给邻居节点。每个节点不但自己监测入侵，也综合邻居节点传入的入侵信息，形成全局入侵响应。

分层结构IDS典型层次如图 1 所示[3]，整个MANET系统按簇为单位分成多IDS簇，每个簇选出簇头，IDS功能模块按层次划分分别位于簇头和簇成员节点上。IDS系统层次分为 2 层或者更多层次。

分层结构的最大优点是网络的可扩充性好，网络和 IDS 的规模不受限制，路由和控制开销比平面结构小，可按层次分解 IDS 系统功能模块，实现分布式多监测器检测入侵、集中管理的机制。

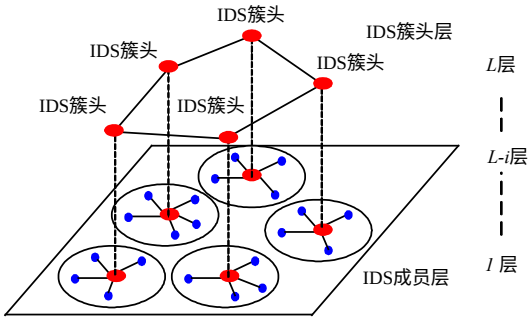

图 1　分层结构 IDS 层次

1.1　加权分簇 IDS 模型

针对 MANET 网络结构，笔者提出了一种加权选簇的分层 IDS 模型。建立层次型网络结构模式的关键问题是要对平面网络进行分簇，以簇头节点为中心构成分层结构，并将网络中的节点分配到不同的簇中，生成层次型的移动自组网。在分层模型中，IDS 簇成员节点执行监控模块，主要进行网络监控和主机监控。每个节点上都要运行基于主机的代理，作为系统入侵检测的探测器。IDS 簇头执行判决模块，收集通信范围内的监控模块传来的数据包并对它们进行分析，用于判断网络是否受到攻击。

分簇算法可以用在MANET的多个网络层次，比较常见的

作者简介：李胜广(1977－)，男，博士研究生，主研方向：无线通信，信息安全，嵌入式系统等；刘建伟，博士、副教授；张其善，博士生导师、教授
收稿日期：2006-11-15　**E-mail：**lishengg@ee.buaa.edu.cn

是基于分簇结构的路由协议[4]，比如CBRP, CEDAR, ZRP等协议。本文将分簇算法应用于IDS簇头选择过程中，属于MANET应用层的范畴。分层IDS模型中分簇算法和工作机制与基于分簇结构的路由协议没有直接关系，它们应用的层次不同，二者互不影响，自成系统。

IDS 监控模块运行于网络中每个簇成员节点上，进行本地监测和入侵响应，并及时向 IDS 簇头报告入侵事件。IDS 簇头判决模块根据本机的本地入侵响应和整个簇里面的成员报告上来的入侵事件进行统一审计。若判断的确发生了入侵，则广播发送全局入侵响应消息给簇成员，激发多节点的协作防护，将入侵节点隔离到网络拓扑外。簇节点并将该簇的入侵检测广播到其他簇头，工作原理见图 2。

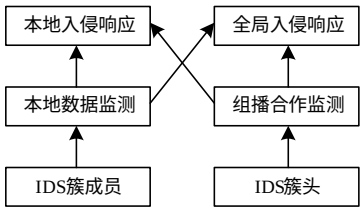

图 2　IDS 代理工作原理

该方案具有以下优点：

(1)充分考虑到节点以及网络安全性指标，使得系统安全性最大；

(2)利用分簇的方式使得该方案适应于较大规模的网络，减轻 IDS 消息广播带来的网络负载；

(3)该方案选出的簇头与网络管理或者分簇的路由簇头并不要求完全一致。IDS 分簇具有独立性。IDS 的簇头尽量和网络管理的分簇簇头分离，可减少簇头的能量消耗。

同样该方案具有以下缺点：

(1)簇头能量消耗比较快，影响整个网络的寿命。

(2)权重参数选择比较困难，参数选择不当可能会造成网络稳定性的瓶颈。

1.2　加权分簇算法

利用加权分簇算法进行簇头选择，每个节点分配一个权值指示该节点适合充当 IDS 簇头的程度。各节点的权值可以使用一个考虑多种因素的通用公式表示：

$$W = \alpha * Capacity + \beta * Security$$

$$Capacity = a * Mb + b * Dg + c * Pw + d * En$$

$$Security = e * Ph + f * Ih + g * Is$$

其中，*Capacity* 表示节点本身的网络能力，主要由本地特性参数组成，*Mb* 表示节点的速度或相对邻居节点的移动性，*Dg* 表示直接连接的节点数的节点度；*Pw* 表示节点的传输功率；*En* 表示节点剩余的能量参数；*Security* 表示节点本身的安全能力，它由安全参数决定；Ph 为物理安全指标；*Ih* 为入侵检测历史指标；*Is* 为入侵检测当前速度；加权参数 α , β ,*a*,*b*,*c*,*d*,*e*,*f*,*g* 根据网络系统的要求动态调整。

加权选簇算法的簇头选择过程包括下面步骤：

(1)初始化时所有节点处于完全分散状态。每个节点计算自身的安全能力参数 *Security*。*Ph* 可以由本地系统是否具有强健的安全保护措施确定，比如操作系统和它的补丁、系统登录密码的长度等计算得出，最后归一化处理。*Ih* 为入侵检测的历史指标，利用该节点已经检测的入侵事件的次数来表示。采用其负值，表示该参数与 *W* 呈反向增长关系。*Is* 为入侵检测当前速度，利用当前入侵事件的次数与整个网络通信的数据包的次数相比的值表示，也采用其负值。

(2)节点周期性地交互“ Hello ”信息确定各自的邻居节点数，作为其节点度。计算每个节点的平均速度，采用它的负值作为 *Mb*。根据节点到所有邻居节点的距离之和 *Pw* 作为节点的传输功率。根据节点的剩余电池量和发射功率的比计算出 *En*。

(3)每个节点计算组合权重 W，其中，$\alpha+\beta=1$; $a+b+c+d=1$; $e+f+g=1$。组合权重的值越大的节点越适合充当 IDS 簇头。

(4)将节点的组合权重 W 和其节点 ID 号放置在周期性的“ Hello ”探测消息中广播到邻居节点。相邻节点中具有最大 W 的节点充当簇头。如果 W 相同，则采用其 ID 最小的节点作为簇头。簇头节点广播一个簇头胜选消息，第 1 次收到该消息的邻居节点将成为该簇头所在簇的成员节点，并且它通过广播一个分簇消息宣布自己是该簇的成员节点，而不再参与分簇，

(5)重复上述步骤，直至所有的节点属于某个簇。

簇结构形成之后，簇内的成员节点需要监视收到的来自簇头的信号强度，如果信号强度低于一定的阈值时，节点通知簇头它将离开该簇，然后设法加入其他邻居簇，同时簇头相应地更新其成员列表。

2　告警消息保全传递

2.1　簇头密钥分发

文献[5]中提出了一种被称为“ 复活鸭子 ”的密钥管理模型，它提出每个节点初始化(被比喻成小鸭出生)时，都将第 1 个通过安全信道发送密钥给它的节点认作母节点，它在整个生命周期内只受母节点控制，母节点通过一个访问控制列表来告诉子节点可以和谁进行对话。这种状态一直持续到子节点“ 死亡 ”。节点死亡后才能被重新复制，才能有新的母节点。每个节点的密钥都是由它的母节点产生并分发，节点的身份也只能由母节点识别。整个安全链是一个分层的主从结构的树型拓扑。

从“ 复活鸭子 ”模型中得到启发，对于本文加权分簇的分层 IDS 模型，对这种模型进行改进。首先节点进行选簇，选簇结束后，簇头静态地作为节点的母节点；如果有新节点加入网络，那么它将新进入簇的簇头作为其母节点。分簇结构的 IDS 映射到平面图上，即为树结构，采用改进的复活鸭子模型非常适合这种分簇 IDS 系统。通过这种模型，簇头会获取到它本簇所有节点的共享密钥和其他簇头的公钥。

这种方法对节点的计算能力要求不高；消耗网络资源少；单个节点失效对于整个网络安全性的影响有限。缺点是如果簇头失效，则它所控制的下面子树的所有节点都会失效。

2.2　告警信息签名

哈希函数与各种加密算法有着密切的关系，被广泛地应用于数字签名、消息的完整性鉴别、消息的起源认证等。另外也和各种密码算法一起构成混合密码系统。哈希函数的模型为 $h=H(M)$。其中，*M* 是待处理的明文，可以为任意长度；*H* 是哈希函数，*h* 是生成的报文摘要，它具有固定的长度，并且和 *M* 的长度无关。单向哈希函数具有下列性质：

(1)给定 *M*，很容易计算 *h*；

(2)给定 *h*，找到 *M* 在计算上是不可行的；

(3)给定 *M*，要找到另一消息 *M'*并满足 $H(M) = H(M')$ 在计算上是不可行的；

(4)找出两条随机的消息 *M* 和 *M'*在计算上是不可行的。

如果满足了前 3 条，称之为弱哈希函数；4 条都满足的话，称之为强哈希函数。

在告警完整性保护的时候，需要用到单向哈希函数和消息鉴别码技术。在数据传递过程中，可以采用数字签名技术来同时验证数据的真实性、完整性和发送者。数字签名基本原理如下：

(1)告警信息采用哈希算法进行运算，得到一个固定长度的数字串，称为报文摘要(message digest, MD)，不同的告警报文所得到的报文摘要各异，但对相同的告警报文它的报文摘要却是唯一的。

(2)发送方生成报文的报文摘要，用自己的私钥对摘要进行加密来形成发送方的数字签名。

(3)这个数字签名将作为报文的附件和报文一起作为 P 发送给接收方。即

$$P = F(Es(MD), M)$$

其中，$MD=H(M)$；M为告警信息；E_s为签名函数；F为告警打包函数。

本文根据 MANET 中 IDS 告警需要传递的信息设计了告警信息数据包的格式，如图 3 所示。源 ID 表示发送该数据包的节点号，利用硬件地址表示。包含入侵的 ID 和所属簇的 ID 为了通知其他簇头和直接所属簇头，进行全局的隔离，防止进一步的网络损害。

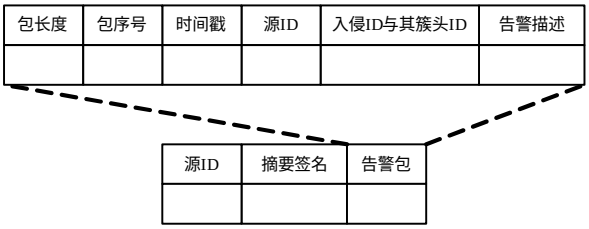

图 3　IDS 告警包组成结构

(4)接收方首先从接收到的原始报文中用同样的算法计算出新的报文摘要，再用发送方的公钥对报文附件的数字签名进行解密，比较两个报文摘要，如果值相同，接收方就能确认该数字签名是发送方的。

通过数字签名，可以达到:

(1)可以向接收簇头保证，信息的确是来自声明的发送簇头，并且实施了认可措施，也就是排除了声称信息是伪造的发送者。

(2)可以向接收簇头保证，信息在发送簇头和接收簇头之间传输的过程中，没有被改变。

ASCII 字符串通常采用 ELFhash 函数作为哈希函数，ELFhash 函数被认为具有均匀散布特性。举例说明告警消息 M 字符串的格式见表 1。

表 1　IDS 告警包举例

长度	序号	时间戳	源 ID	入侵 ID 与其簇头	告警描述
73	1235	060428211625	00E04D114CA6	00F425136ABD-00FABD0E04DD	Routing message error

告警字符串使用其 ASCII 码值，参见下面代码：

unsigned int ELFhash(const char *alertData,unsigned long hashSize)

```
{register unsigned int hash = 0;
unsigned int x = 0, i=0;
unsigned int aiLen=strlen(alertData);
for(i = 0; i < aiLen; i++) {
//左移四位，进行 ASCII 值相加
hash = (hash << 4) + alertData [i];
//高 4 位是否有值
if((x = hash & 0xF0000000L) != 0) {
//高 4 位移至第一个字节的高 4 位，并异或
hash ^= (x >> 24);
hash &= ~x;}
}
//返回哈希表的位置
return (hash & 0x7FFFFFFF) % hashSize + 1;
}
```

发出者簇头计算 ELFhash 函数的结果，表 1 所计算的消息签名 MD 为 5814(HashSize 采用 9999)。再利用发出者的私钥加密 MD，发给其他簇头，接收簇头收到后根据其公钥认证签名，并且如果没有错误，可用其数据包中的源 ID 再一次验证发出者。然后将哈希出来的结果利用发出者的私钥进行数字签名，确保这条记录在传递过程中没有被入侵者篡改或者其他修改。这样当告警信息传递到其他簇头时，接收簇头分析包中的数据，获取到源簇头节点的 ID，根据其已经获取到的源节点的公钥解密数字签名部分，与实际的告警信息比较，进行签名验证。如果正确则接收进行下一步的防护措施，如果错误则主动向源簇头发送错误询问消息，进一步核实是否发生了入侵。

3　结束语

利用加权分簇算法的分层 IDS 充分利用分层 Ad Hoc 的网络优势,有利于 IDS 本地模块与全局模块之间的信息交互。本文详细说明了在这种分层 IDS 结构中的告警消息如何正确地传递到其他簇头，保证整个网络系统及时广播制裁措施隔离入侵节点的一种方案，利用哈希函数和签名技术对簇头之间的 IDS 入侵告警信息进行数字签名,计算和内存消耗较小，适合移动自组网资源受限的特点，非常适合自组网网络安全防范的应用。

参考文献

1 IEEE 802.11. Standard Specifications for Wireless Local Area Networks[EB/OL]. (1999-11). http://standards. ieee.org/wireless/.

2 Luo H, Zerfos P, Kong J, et al. Self-securing Ad Hoc Wireless Networks[C]//Proc. of the 7th IEEE Symposium on Computers and Communications. 2002.

3 郑少仁. Ad Hoc 网络技术[M]. 北京: 人民邮电出版社, 2005-01.

4 Zhu Yuan, Chen P, Liestman A L, et al. Clustering Algorithms for Ad Hoc Wireless Networks[M]. [S.l.]: Nova Science Publishers, 2004.

5 Stajano F, Anderson R. The Resurrecting Duckling: Security Issues for Ad Hoc Wireless Networks[C]//Proc. of the 7th International Workshop on Security Protocols. 1999.