DOI:10.13374/j.issn1001-053x.2007.s2.100
第29卷 增刊2 北京科技大学学报 Vol.29 Suppl.2
2007年 12月 Journal of University of Science and Technology Beijing Dec. 2007

基于Agent的安全协议对抗Ad Hoc网络下的拒绝服务攻击

陈红松 王昭顺 宁淑荣

北京科技大学信息工程学院计算机系，北京 100083

摘 要 拒绝服务攻击是Ad Hoc网络安全领域中的难题，本文提出一种新型的基于Agent的安全路由协议，Agent可根据其邻节点的可信度定期更新以适应Ad Hoc分布式路由计算环境，有效提高网络的可信性，降低网络安全计算的复杂度；根据拒绝服务攻击的特征抽取出Agent安全规则与检测算法．采用NS2网络模拟器的仿真结果表明，该方法能有效的检测出拒绝服务攻击并进行及时响应，使网络性能迅速恢复正常．

关键词 Ad Hoc路由协议；智能体；入侵检测；网络安全

分类号 TP393.08

Ad Hoc网络技术是近年来十分活跃的研究领域，该网络结构不依赖于现有的网络基础设施，由移动节点组成的临时性自治系统，具有自组织、自适应、无中心、多跳通信、动态变化的拓扑结构等特点．可应用于军事通信、紧急搜救、智能大厦、智能家居、航天深空探测设备通信等重要领域，有着巨大而广阔的应用前景[1-3]．

作为一种无线移动网络，Ad Hoc网络和传统的移动网络有着许多不同，其中一个主要的区别就是Ad Hoc网络不依赖于任何固定的网络设施，每个移动节点既是终端又是路由器，能够提供包的存储转发功能．通过移动节点间的相互协作来进行网络互联．由于无须固定通信设施的支持，因此，无线自组织网络具有很高的可靠性和灵活性．但是正是由于这种网络的特点，使得Ad Hoc网络的安全问题尤为突出，其安全问题和安全策略便日益受到重视．它相对与传统网络更容易受到攻击，而且防范更加困难．在传统网络中，网络采用层次化的体系结构，具有相对稳定的拓扑．传统的集中式网络管理模式，包括相关的安全策略，如加密、认证、访问控制和权限管理、防火墙、入侵检测等，适合稳定的网络环境和应用程序，但面对移动Ad Hoc网络等新兴应用则缺乏智能、主动和动态的信息处理能力．相比之下，自组网由于节点的移动性和网络拓扑结构的动态变化，不具有上述网络功能，从而导致传统网络中的安全机制不再适用于自组网．网络内部的节点因缺乏足够的保护很可能被攻击、占领而导致网络瘫痪．因此研究新的适合于自主网的安全协议具有非常重要的理论和现实意义．

收稿日期：2007-09-01

作者简介：陈红松(1977－)，男，讲师，博士

1 AODV路由协议简介

AODV (Ad Hoc on demand distance vector routing)是一种典型而又重要的Ad Hoc网络按需路由协议，只当源节点需要往目的节点发送数据时才发起路由过程[1]．AODV路由协议以其网络开销、算法复杂度等大部分性能指标优于其它同类而受到广泛关注，被认为是最有实用前景的Ad Hoc网络路由协议之一，目前已被IETF标准化．本研究针对AODV路由协议进行安全性方面的研究，探讨了该协议存在的安全问题和漏洞．并在分析和对比各种已有安全策略的基础上提出了一种基于Agent的入侵检测及响应机制．

2 Ad Hoc及AODV路由协议的安全研究现状

早期的安全Ad Hoc路由协议使用公钥管理系统来保护Ad Hoc路由消息．Capkun等提出了异步的、分布式密钥管理策略[2]．采用加密机制如数字签名来保护路由信息和数据交换．每个节点都有一个公有/私有密钥对，所需的密钥管理服务由一组节点来完成．管理的实现采用了阀值加密算法(n,k)表示在n个节点的网络中，任何$\geqslant k$个节点的集合都能够执行加密操作；反之任何$<k$个节点的集合则不可以．该策略还采用了私有密钥定时更新的方

法，使攻击者很难同时获取到 k 个节点的有效密钥. 然而，由于公共密钥繁重的计算量，该协议对于 Ad Hoc 网络中节点计算的代价过大.

美国 CMU 大学的 Hu、Perrig 和 Rice 大学的 Johnson 等提出用数字签名来保障路由协议的安全性. 文献[3]中提出了一种基于 DSR 的安全按需路由协议—Ariadne.

SEAD 是 Hu、Johnson 和 Perrig 提出的一种基于距离矢量路由协议 DSDV 的安全路由协议[4]. 通过让哈希值和路由信息中的权值以及序列号相关联，使用单向哈希函数来防止恶意节点减小路由信息中对应目的节点的权值或者增加它的序列号.

我国国防科大的况晓辉、卢锡城等提出移动自组网络分布式组密钥更新算法——CDGR (cluster distributed group rekeying)算法[5]，该算法能够利用局部密钥信息更新组密钥，适合拓扑结构变化频繁、连接短暂且带宽有限的移动自组网络. 采用 NS2 模拟器验证了算法在移动自组网络中的有效性. 但是当节点加入或退出过于频繁时，将导致组密钥过度更新，从而造成网络拥塞，如何利用定时更新机制解决移动自组网络中组密钥过度更新的问题仍然需要进一步研究.

我国清华大学的林闯教授等提出可信网络的概念[6]：过去的研究以追求高效行为为目标，而今天的计算机系统需要建立高可信的网络服务，可信性必须成为可以衡量和验证的性能. 文章指出无线移动环境下的网络可信性问题面临着更严重的威胁，相关的代表性工作主要有可信传感器网络、Ad Hoc 网络的信任评估和移动 IPv6 的信任管理. 可见提高 Ad Hoc 网络的安全及可信性研究是目前网络安全领域研究的重要内容.

都柏林大学的 Elizabeth Gray 教授提出了 Ad Hoc 网络下的可信计算框架[7]. 作者指出信任是所有人际关系的基础，该策略模仿人类社会中人际关系的信任建立过程，并依据信任度来进行局部的基于角色的访问控制. 可信框架包括执行的检查、可信度的计算与存储、信息交互的监督、动态访问控制、可信计算的形式化等，文中以无线 Ad Hoc 网络中的扑克牌游戏为示例介绍了该框架的可行性. 该方案的缺点是没有针对 Ad Hoc 网络设计节点可信度的定量的评估方法.

3　AODV 路由协议下拒绝服务攻击的形成过程

由 AODV 路由协议的运行机制可知，路由请求报文 RREQ 和路由应答报文 RREP 在路由的建立过程中起重要作用，所以恶意节点主要针对这两种报文进行伪造以达到攻击目的. 在本研究过程中恶意节点采用主动伪造数据包进行拒绝服务(DoS)攻击.

拒绝服务 DoS(denial of service)攻击指使节点无法提供对其他合法节点所需的正常服务，它能够在自组网的各层进行. 在物理层和 MAC 层，攻击者通过拥塞无线信道来干扰通信；在网络层，攻击者能破坏路由信息，使网络无法互连；在更高层，攻击者通过伪造使高层服务紊乱. 本文主要针对由 RREQ 泛洪引起的拒绝服务.

在 RREQ 泛洪攻击中，一个攻击节点可以通过广播大量伪造的 RREQ 消息占用网络带宽，消耗其它节点的计算和存储资源，使网络连接几乎中断. 如图 1 所示.

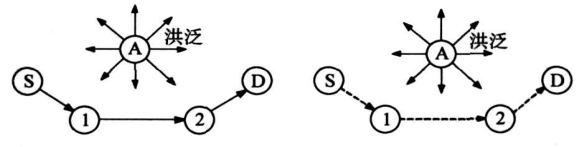

图 1　由恶意节点进行 RREQ 泛洪造成的攻击. (a) 泛洪攻击前；(b) 泛洪攻击后

由图 1 可知，恶意节点 A 不断的发出大量的伪造 RREQ 路由请求广播信息进行泛洪攻击，其它节点对突然出现的大量 RREQ 进行检查与应答，泛洪对其它节点的存储和计算资源带来了巨大的冲击，消耗了大量的传输带宽，使源节点 S 到目的节点 D 的网络连接几乎中断.

4　基于智能 Agent 的安全路由协议描述

由 Ad Hoc 网络安全研究现状可知，采用加密等传统的安全机制对 Ad Hoc 网络计算复杂度过大；采用集中式安全控制则中心节点容易受到攻击而导致瘫痪，容错及容侵性能比较差；而 Wenke Lee 的完全分布式安全机制则要求每个节点都参与安全协议，如果有 N 个节点，则计算及存储代价随 N 线性增加——代价过大. 本研究提出了基于智能 Agent 更新的安全扩展协议，充分吸收了现有安全机制的优点，又克服其缺点.

Agent 技术是目前计算机科学领域中一个非常重要、研究活跃的内容之一，特别是近年来随着计算机网络技术的发展和广泛应用，Agent 技术引起了学术界和工业界的高度关注和重视. 本研究将 A-

gent 技术应用于 AODV 安全路由协议设计里，提出了一种新型的基于 Agent 更新的安全检测及响应算法，能有效针对以上两种典型攻击进行检测及响应，显著提高协议的安全性能. Agent 在人工智能领域被称为智能代理或智能主体，它具有以下特征.

(1) 自主性，亦称自治性. 即能够在没有人或别的 Agent 的干预下，主动地、自发的控制自身的行为和内部状态，并且还有自己的目标或意图.

(2) 反应性. 即能够感知环境，并通过行为改变环境.

(3) 面向目标性. 一个 Agent 有能力处理复杂和高水平的任务，它应该自己决定如何将任务很好地分解并处理为多个小的子任务，以及这些子任务处理的顺序和方法等.

(4) 适应性. 即能根据目标，环境等的要求和制约做出行为计划，并根据环境的变化呈现灵活解决问题的行为，修改自己的目标和计划.

Agent 作为智能化主体可以根据网络运行情况改变自身状态. 为了避免 Agent 本身如果受到攻击以及单一 Agent 节点执行安全检测算法而过早耗尽电能，本研究提出 Agent 动态转换及更新的新机制：Agent 不仅执行协议代码、收集数据，而且还有自己的动态生命状态；由于 AODV 是按需路由协议，只有在源节点需要向目的节点传输数据时才发起路由请求，Agent 随路由的建立而建立，随路由的完成而释放，随路由请求—应答流的状态变化而动态的产生、执行、更新与消亡. 因此，网络里有多少个路由请求—应答流，也就对应多少个 Agent 来进行实时的安全检测与响应.

安全协议每隔一段时间探测网络中是否有路由请求—应答流产生，如果没有数据包传输，说明现在网络相对稳定，不需要进行安全检测，也就没有 Agent 产生；如果有路由请求—应答流产生，则在源节点和目的节点之间随机选择一个节点作为 Agent 执行安全路由协议；经过一段时间周期后，如果该流中仍然有路由请求—应答包，Agent 将从它的邻居节点列表中选取一个可信度最高的邻居节点作为网络中下一个安全 Agent 来更新替换现在的 Agent，并将会话树列表拷贝到新的 Agent 中，使每一个可信度高的邻节点都有机会成为安全 Agent 来执行安全协议，同时也平摊了执行网络安全检测带来的计算开销；由于每个流对应一个安全 Agent，其计算及存储代价比完全分布式安全协议大大减少，通过 Agent 定期更新也降低了 Agent 本身被恶意攻击的概率，以此来保证 Agent 本身的公平和安全性. 节点可信度的确定是根据数据包被节点成功转发的概率来决定的，即成功转发率越高，节点的可信度也越高.

智能化的 Agent 创建及更新机制能适应 AODV 分布式路由计算环境，通过构造会话树列表对路由请求 RREQ 和路由应答 RREP 流进行实时跟踪与统计，不断的建立、查找与更新会话树列表，根据其方向和数据的一致性进行安全性能分析，通过对所有流的监测达到对整个网络的监测，并根据 Agent 中的安全检测算法进行攻击的检测及响应. Agent 可以根据网络和邻节点的信息来动态规划下一个新的 Agent 以替换当前 Agent，由于新的 Agent 是原 Agent 的邻居节点，会话树列表的拷贝和转换速度很快. 在任一时刻，网络中每一个流对应一个 Agent 执行安全协议，而在一段连续时间内则有多个高可信节点轮流作为 Agent 执行安全协议，相当于 Agent 里的智能化检测与响应程序在不同高可信节点上分布、分时的运行，既满足了自组织网络的开放特征，又保证了系统的安全性.

在基于 Agent 更新的安全协议中作了以下假设：(1) Agent 一开始是位于源节点和目的节点之间的一个随机选择的内部节点，随着时间变化定期进行更新，它有能力访问其它节点的路由表. (2) Agent 可以侦听并获取它所对应路由请求—应答流的路由信息，对获取的信息进行智能处理，并且有能力对节点进行安全访问控制. (3) Agent 根据安全目标执行特定的任务. 根据需要在高可信节点间移动，可将一个流的安全计算负荷分散到网络的多个高可信节点上，使小系统具有处理大规模、复杂问题的能力.

基于 Agent 的安全机制如图 2 所示.

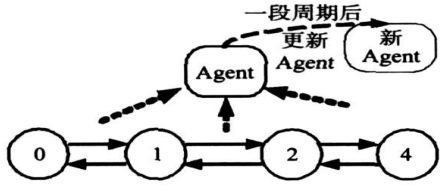

图 2 基于 Agent 的安全机制

由于一个 AODV 路由请求—回复流可以被源 IP 地址、目的 IP 地址和广播 ID 号唯一的鉴别，源和目的序列号分别在请求和应答过程中保持不变，Agent 可以由它们来建立会话树列表表头以标示一个路由的建立，为了对 RREQ 泛洪进行检测，在会话树列表里增加了单位时间内的源节点发出的 RREQ 个数——RREQCount，为泛洪的检测提供了有效的检测数据.

Agent 针对 RREQ 路由请求消息的安全检测及响应算法如图 3 所示.

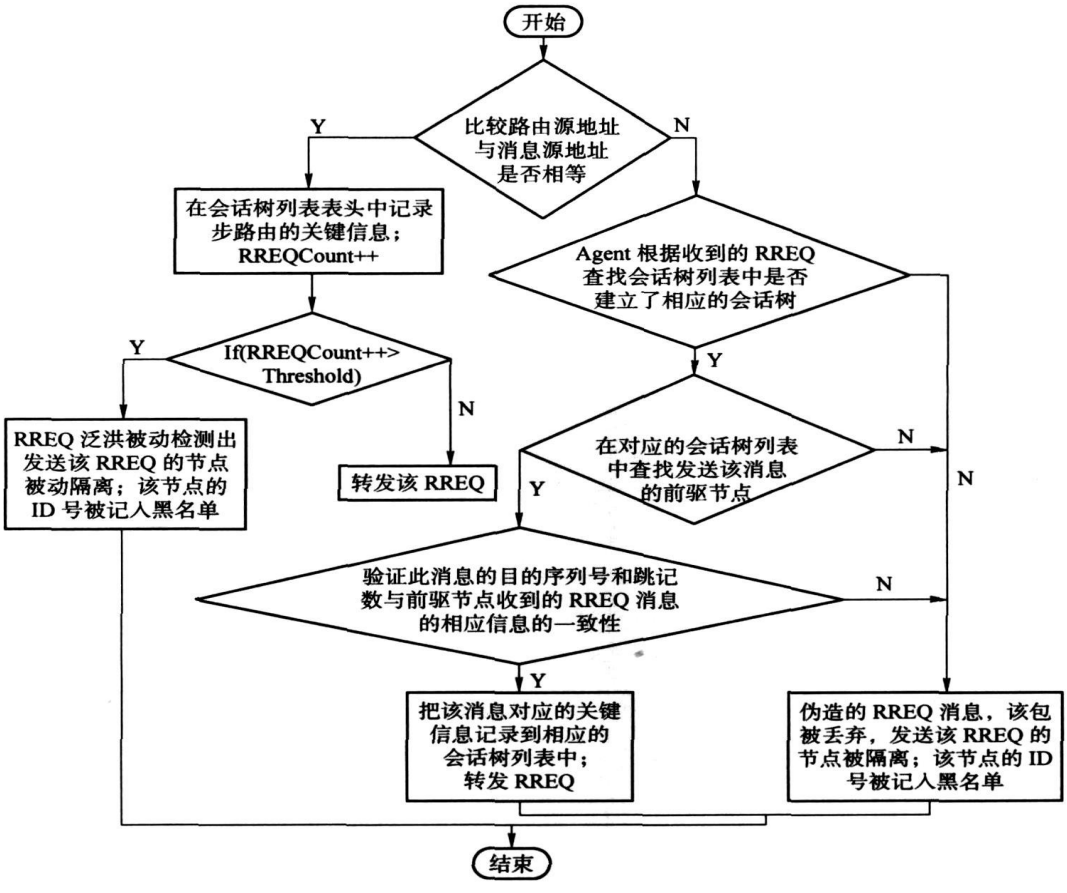

图 3　基于 Agent 的入侵检测及响应算法

当节点收到一个 RREQ 节点时，Agent 首先比较发送这个消息的节点地址和路由源地址是否相等. 若相等，则建立这个新发起路由的会话树的表头，并在此表头中记录此次路由的源地址、目的地址、广播 ID、源序列号等关键信息. 用于记录源节点发送 RREQ 数目的 RREQCount 值加 1，如果 RREQCount 大于阈值，则 Agent 判定这次路由请求是RREQ 泛洪，通过发送包含该节点目的 IP 地址不可达的 RERR 消息使发送该 RREQ 的节点被隔离，该节点的 ID 号被记入黑名单. 如果 RREQ-Count 小于阈值，则正常转发该 RREQ 消息. 由于网络中的节点数目会随着节点的加入和退出而动态变化，每隔一段时间安全协议将通过安全 Agent 发出活动节点探测包，获得当前网络中活动节点的数目 N，并将 RREQCount 阈值设为($N-1$)；因为在单位时间内，除了发送此 RREQ 消息的源节点外，当前最多只能有($N-1$)个节点接受到该消息，从而实现了泛洪检测阈值的动态设定.

5　仿真与分析

5.1　仿真环境的建立

利用 NS2 网络仿真平台，对 AODV 的攻击及安全改进算法进行仿真. 使用 Tcl 语言对网络场景进行配置，定义了诸如各个移动节点的网络物理接口类型、天线类型、无线射频参数、无线电波传输范围、媒体访问控制层(MAC)使用协议、移动场景文件、通信场景文件，移动节点类型及数目、仿真时间等.

模拟参数如表 1 所示，暂停时间为节点两次运动之间的停留时间。

从表 1 中可以看出，本次场景在 1 000 m × 600 m 的范围内有 20 个节点，建立了 5 对通信连接，通信节点每秒发送 4 个分组，节点的通信半径为 250 m. 本次模拟总共持续时间是 300 s.

5.2　仿真结果及性能评价

由于每次仿真结束后均生成 Trace 文件来记录仿真过程，通过对该文件的分析就可以得到网络的

表 1 模拟参数

参量	类型及数值
业务流类型	CBR
媒体访问控制	802.11
节点个数	20
仿真区域	1 000 m×600 m
仿真时间	300 s
暂停时间	2 s
分组速率	4 pkt/s
连接数目	5
传输范围	250 m
数据链路带宽	2 Mbps
攻击节点数目	1

关键性能度量指标，如分组转发率、平均传输速度等，并根据拒绝服务攻击里泛洪和环路攻击的特征而定义了一些新的性能评价指标. 由于在泛洪攻击里 RREQ 数目急剧增加，分组转发率则急剧下降，本文以此作为对泛洪检测算法评价的度量指标，仿真结果如图 4 所示.

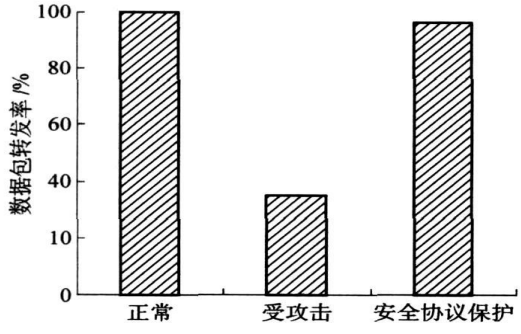

图 4 路由泛洪攻击及防御结果

由图 4 可知，在正常情况下分组传输率为 100%，受到 RREQ 泛洪攻击后，网络受到大量 RREQ 广播的冲击导致网络拥塞使部分包丢失，分组传输率下降到 38%，而在 Agent 的安全协议下分组传输率又恢复到 98%，接近正常水平，可见由于 Agent 里的安全检测算法通过对请求(应答的跟踪统计，并与 RREQCount 阈值进行比较，及时检测到泛洪攻击并对恶意节点进行隔离，使网络免受 RREQ 泛洪攻击的危害，网络的性能迅速恢复到接近正常水平，通过实验验证了本研究提出的安全协议的正确及有效性.

6 结论

Ad Hoc 网络通过无线信道在节点间通信，传送的信息非常容易受到篡改、伪造等各种攻击，网络安全问题更加突出.

(1) 本文提出了一种基于 Agent 更新机制的 AODV 安全路由协议，每个 Agent 对应一个路由请求(应答流. Agent 本身具有动态的生命周期，有多少个流就有多少个 Agent 实时跟踪路由请求(应答流. 该安全性扩展协议在原有的 AODV 路由协议的基础上通过 Agent 构造一个与该流对应的会话树列表. 根据攻击特征抽取出 Agent 安全规则，Agent 根据智能检测算法和安全规则检验网络中 RREQ、RREP 消息的合法性，动态设定泛洪检测阈值，动态建立和更新相应的会话树，以到达检测攻击、及时响应的目的.

(2) 基于 Agent 的安全机制中，本文首次提出了节点可信度的概念，使 Agent 邻居节点里可信度高的节点有机会成为新的安全 Agent，也使安全 Agent 可以在自组织网的多个可信节点之间分布、分时运行，比单纯的集中式安全方案提高了容侵性，比完全分布式安全方案降低了计算复杂性、提高了网络可信性，既适应了 Ad Hoc 网络的动态多跳特征，均摊了安全检测的计算代价，又保证了 Agent 本身的公平及安全性.

本文对 AODV 路由协议的攻击、安全机制的分析与研究及定量性能评价，对于 Ad Hoc 网络将来的安全性改进及应用具有一定的理论和现实意义.

参 考 文 献

[1] Perkins E S. Ad Hoc on-demand distance vector (AODV) routing (Internet draft). http://moment.cs.ucsb.edu/AODV/draft-ietf-manet-aodv-13.txt, 2003

[2] Capkun S, Buttyan L, Hubaux J. Self-organized public-key management for mobile Ad Hoc networks. **IEEE Transactions on Mobile Computing**, 2003, 2(1): 52

[3] Hu Y, Perrig A, Johnson D B. Ariadne: a secure on-demand routing protocol for Ad Hoc networks//Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom '02), Atlanta, 2002: 12

[4] Hu Y, Johnson D B, Perrig A, SEAD: secure efficient distance vector routing for mobile wireless Ad Hoc networks // Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02), Washington DC, 2002: 3

[5] 况晓辉，朱培栋，卢锡城. 移动自组网络分布式组密钥更新算法. **软件学报**，2004，15(5)：357

[6] 林闯，彭雪海. 可信网络研究. **计算机学报**，2005，28(5)：751

[7] Gray E, Jensen C. Trust evolution policies for security in collaborative Ad Hoc applications. **Electronic Notes in Theoretical Computer Science**, 2006, 157(3): 95

Agent-based security protocol against DoS attack in Ad Hoc network

CHEN Hongsong, *WANG Zhaoshun*, *NING Shurong*

Department of Computer Science, School of Information Engineering, University of Science and Technology Beijing, Beijing 100083, China

ABSTRACT Denial-of-Service (DoS) attacks are the main puzzles in the security of Ad Hoc network. A novel agent-based security routing protocol scheme was proposed to block DoS attacks. Agent can update itself at some interval by the trustworthiness of the neighbor nodes to fit the Ad Hoc distributed routing computing environment. It can efficiently improve trustworthiness and decrease computing complexity. Agent security specifications were extracted by the feature of the attacks. NS^2 simulator is expanded to validate the security routing protocol. Simulation results show that agent-based security scheme is highly effective to detect and block DoS attacks.

KEY WORDS Ad Hoc routing protocol; agent; intrusion detection; network security