第 33 卷 第 9 期 计 算 机 工 程 2007 年 5 月
Vol.33 No.9 Computer Engineering May 2007
·安全技术· 文章编号：1000—3428(2007)09—0140—02 文献标识码：A 中图分类号：TP309

# MANET 中隧道攻击的研究与实现

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：**目前 MANET 中安全方面的研究大多是对单个节点实施的恶意行为的分析和防范。该文研究了一种多节点配合的攻击模式——隧道攻击。结合 DSR 路由协议和 NDM 安全模型验证了隧道攻击的有效性和对网络的危害性，提出了设计相应安全措施的方向。
**关键词：**移动自组织网络；安全；隧道攻击；入侵侦测

# Study and Implementation of Tunnel Attack in MANET

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

**【Abstract】** Most recent security-related research on Ad Hoc network focuses on malicious nodes which do the misbehavior alone. This paper details a collaborated attack method——tunnel. Through simulation based on the DSR routing protocol and NDM security method, it shows that the tunnel attack is feasible to take considerable intrusion effect even the NDM is enabled. The corresponding security advice is given in the conclusion based on the evaluation results.
**【Key words】** Mobile ad hoc network(MANET); Security; Tunnel attack; Intrusion detection

## 1 概述

移动自组织网络(Mobile Ad Hoc Network, MANET)开放信道、动态拓扑、协作路由的特点决定了它特别容易受到攻击。同时，使传统的基于中心的安全防范措施也很难适用。

MANET 安全系统的设计，首先必须分析系统可能存在的安全漏洞，研究可能的入侵行为。MANET 处于 P2P 工作模式，对网络的安全威胁是复杂的、多样的。只有对各种攻击行为进行细致的研究，总结出它们的行为特点和攻击模式，才能据此增强系统的安全防范功能，或设计有针对性的入侵检测系统。在各种攻击行为中，对网络协议和应用层面的攻击是 MANET 网络安全的焦点，攻击的手段大致可分为 3 类：

(1)窃听：指恶意节点通过监听信道，得到其他节点的路由、位置信息。通信如果不经过加密，甚至可以直接监听其他节点通信内容。但监听网络未必就是攻击行为，有些物理层传输协议和MANET的安全措施也要求节点对网络进行监听。由于MANET信道的开放性和监听的隐蔽性，因此这类行为几乎无法侦测，只能通过加强通信的保密性来预防。目前，“不泄漏方法”(NDM)[1]利用基于RSA算法的加密体系可以为用户提供灵活可调的安全性和隐私度，是增强MANET通信保密性的首选措施。

(2)路由破坏：这类攻击利用 MANET 路由协议的逻辑规则，恶意节点篡改路由寻址消息的某些关键字段或发起设计好的恶意寻址过程，引诱其他节点修改路由表，以达到对网络路由的侵入、环路、黑洞、隔离等攻击。

(3)资源耗费：这类攻击的节点通过大量发送无效的寻址请求充斥网络带宽或故意丢弃数据包来降低链路性或实现拒绝服务攻击[2]。

防范后两种类型攻击的手段很多，但本质方法不外乎在路由协议的数据帧中添加额外的验证、加密字段如[2]或设计额外的验证过程如[3]来防止节点的恶意行为。对于这两类的入侵侦测，目前一种使用较广的方式是通过看门狗[4]来发现网络中的攻击行为。

看门狗是基于 MANET 中邻居节点可以互相侦听的事实，通过节点间的互相监视来发现网络中的异常行为。当一个节点发现其邻居没有履行协议规定的下一个动作或者进行了某种攻击的特定动作(如篡改路由寻址信息的关键字段等)就有可能是入侵的行为。

合理结合以上各种安全措施可以增强 MANET 的安全性。然而目前对进攻手段的分析和安全方案的设计大都是针对单个恶意节点的某类攻击行为。像隧道攻击这类多个恶意节点配合实现的入侵手段虽然有所提及，但尚未有系统的研究。

## 2 隧道攻击

隧道攻击的基本思想是网络中恶意节点共同隐瞒它们之间链路的真实距离，引诱其他节点建立经过它们的路由。以此达到吸收网络流量，制造网络拥塞或更进一步的配合其他手段入侵 MANET 的目的。

### 2.1 攻击过程实现

本文以DSR路由协议[7]为例，通过设计如下 6 个步骤实现隧道攻击的全过程：

(1)监听网络：假设网络中有 A、B 两个恶意节点。A、B 通过被动的监听网络中路由发现和数据传输过程，收集自身通向 MANET 中各节点的路由信息 RT(A),RT(B)。

(2)寻找同伴：A 通过广播特定的路由寻址请求 RREQ(A,*)作为接头信号，“*”是隧道攻击约定的某个虚拟的节点。B 发现该 RREQ(A,*)后知道 A 为同伴。然后 B 通过发送路由请求 RREQ(B,A)找到通向 A 的路径，建立隧道链路

**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：**2006-05-20 **E-mail：**cdschen@mail.ustc.edu.cn

link(A,C1,C2,…,Cn,B)。

(3)交换路由表：AB 建立连接后交换各自路由表：RT(A)，RT(B)。

(4)吸收路由：当 A 收到某源节点 S 寻找目的节点 R 的路由请求 RREQ(S,R)时，查找 RT(B)，如果 RT(B)中没有节点 R，按照协议规则正常动作。如果 RT(B)中有通向 R 的链路 link(D,E,…,R)，则发送 RREP 告诉 S 找到路径 link(B,D,E,…,R)。最终，在 S 收到的所有 RREP 当中，如果 link(S,…,A、B,D,E,…,R)的跳数最少，则 S 将其置入路由表。今后 S 于 R 之间的通信都将通过 A、B 之间的隧道进行。

(5)隧道转发：当 A 接到 S 经过 link(S,…,A、B,…,R)发送的数据包时，首先向“邻居”B 转发一次(当然 B 收不到 A 的数据)，但不报告链路中断(link broken)。然后 A 经过隧道 link(C1,C2,…,Cn,B,D,E,…,R)发送原数据包。而 B 通过同样的方式转发 R 返回至 S 的消息。

(6)隧道维护：隧道建立以后，隧道入口节点 A、B 定期交换 RT(A)、RT(B)以吸收更多的路由，并定期检查通向对方的链路情况，保持隧道链路畅通。

### 2.2 攻击手段分析

隧道攻击结合了被动攻击和主动攻击的特征，通过多个恶意节点配合实现对网络路由的重定向侵犯。在隧道攻击中在“监听网络”、“寻找同伴”、“交换路由表”的过程完全使用路由协议提供的正常手段进行；因为“吸收路由”的过程并不篡改其他节点提供的路由信息，而是通过自己的知识引诱网络其他节点建立经过隧道的路由，所以文献[2,3]中的安全增强手段无法阻止隧道攻击。而在隧道转发的过程中节点 A 会正常向“邻居”B 转发数据包，由于 A 的邻居节点(看门狗)无法监听 B 是否能收到 A 的消息，因此隧道攻击也可以躲过看门狗的监控。

隧道攻击每个隧道入口必须有足够的网络节点路由信息才能更多地吸收网络路由，发挥破坏作用。在没有保密措施的路由协议下，进攻节点可以通过任何流经自己的数据的头部路由信息来收集节点信息，而如果网络传输过程采取了保密措施如 NDM，入侵节点就只能通过路由发现时的广播信息收集其他节点信息。而如果 NDM 也应用于路由发现阶段，每个进攻节点就只能收集其相邻节点和与之通信过的节点信息。所以加强网络信息保密性可以通过降低隧道攻击的效果。然而太强的加密如路由发现时也进行加密则会大大降低路由协议的效率。

## 3 仿真结果

本文基于Rimon Barr等人创建的Jist/Swans[5]仿真平台，采用Swans提供的DSR路由协议并实现了NDM作为安全手段，分别模拟了NDM开启和NDM关闭时不同节点运动速度和不同隧道数量下，网络通信经过隧道节点流量的比例(路由吸收率)和发送一条消息的平均转发次数(跳数)，并以此衡量隧道攻击的效果。

Ad Hoc 网络区域为 1 000m×1 000m，100 个网络节点，初始位置均匀分布。节点连续随机移动(Pause time=0)。单个节点通信范围为 200m。每个节点每分钟一次向随机目的节点的通信。NDM 设置：每个节点都是安全代理，对通信内容进行加密,初始状态下密钥已经分发完毕。运行时间为 1 000s。每种设置收集 10 次运行模拟的平均结果。

图 1 结果显示网络中只存在在一对隧道节点条件下，节点移动速度快时网络通信经过隧道节点的平均流量更大。低速或高速，NDM 开启都可以有效地降低隧道路由吸收率。

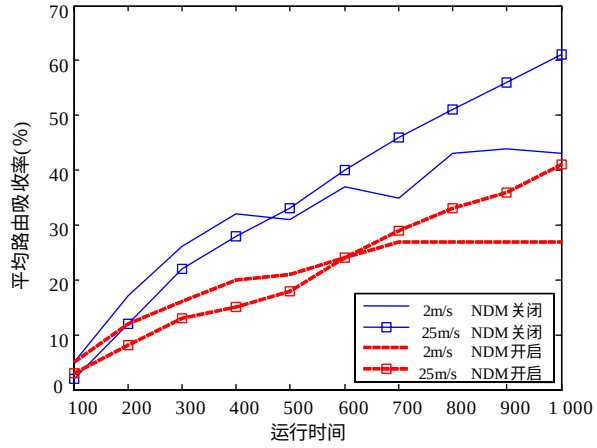


**图 1 固定隧道数(1 条)，不同节点速度(2m/s、25m/s)路由吸收率**

图 2 结果显示网络中只存在一对隧道节点条件下，节点移动速度快时网络发送一条消息需要的转发次数(跳数)更大，即通信时延更大。低速或高速，NDM 开启都可以有效减少隧道攻击引起的通信时延。

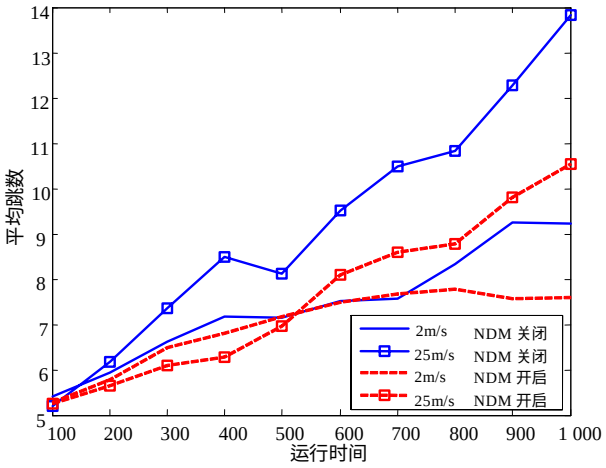


**图 2 固定隧道数(1 条)，不同节点速度(2m/s、25m/s)平均跳数**

图 3 结果显示在同样节点移动速度条件下，隧道数目多时网络通信经过隧道节点的平均流量更大。隧道数目较多时 NDM 开启对降低隧道入侵的路由吸收率的效果很小。

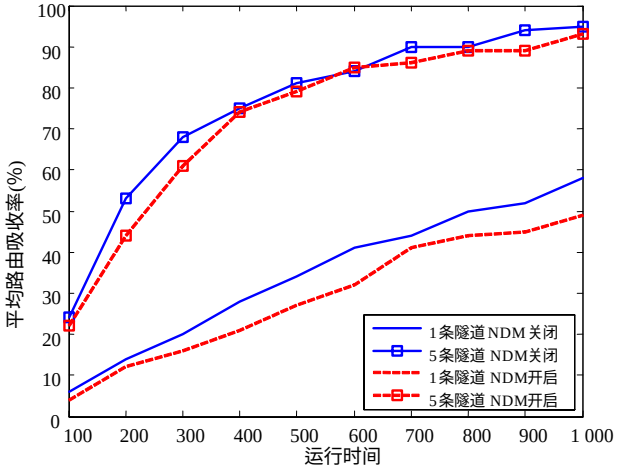


**图 3 固定节点速度(10m/s)，不同隧道数目(1 条、5 条)路由吸收率**

图 4 结果显示在同样节点移动速度条件下，隧道攻击会

（下转第 144 页）