无线移动 Ad Hoc 网络路由协议安全问题分析

蒋 杰 胡光明 窦文华
(国防科技大学计算机学院 长沙410073)

摘 要 Ad Hoc 网络是一种无需固定基础设施的移动自组织通信网络。当前的路由协议没有固有的安全机理,因而面临大量的威胁。本文首先简要介绍了 Ad Hoc 网络和所提出的路由协议,然后详细描述了一些针对路由协议的攻击手段和方法,最后讨论了可能采取的防范措施。

关键词 Ad Hoc 网络,路由协议,攻击,安全路由

Analysis of Security Problems of Routing Protocols for Wireless Mobile Ad Hoc Networks

JIANG Jie HU Guang-Ming DOU Wen-Hua
(School of Computer Science, National University of Defense Technology, Changsha 410073)

Abstract Ad Hoc network is a collection of mobile nodes that communicate without the aid of fixed infrastructures. Current routing protocols have no in-built security mechanism thus face lots of threats. This paper first makes a brief introduction to ad hoc network and some proposed routing protocols. Then it describes in detail some attacks against the routing protocols, followed by some possible defending means.

Keywords Ad Hoc networks, Routing protocol, Attacks, Secure routing

1 概述

Ad Hoc 网络是一种无需固定基础设施的移动自组织通信网络。在某些基础设施被破坏或者不能部署基础设施的场景(比如战场、野外营救等)以及机场、会议等场合,具有广泛的应用前景[11,24]。当前的路由协议设计没有考虑可能遇到的针对路由协议的攻击行为,存在安全隐患。

本文首先对 Ad hoc 网络环境及其主要路由协议进行了介绍,然后详细描述了多种针对路由协议的攻击手段和方法,为下一步设计安全路由协议打下了基础。最后讨论了实现安全路由可能采取的防范措施以及涉及到的关键技术。

2 Ad Hoc 网络环境

Ad hoc 网络是由一组移动节点组成的无线、动态、自组织网络。与传统的移动通信系统(比如蜂窝通信系统和卫星通信系统)必须依赖特定的基础设施不同,Ad hoc 网络由移动节点实现网络的自组织。当两个节点位于无线传输范围之内时,能够实现直接通信;而当两个节点处于无线通信范围之外时,由其他中间节点完成数据转发中继。

Ad hoc 网络的主要特点包括[24]:

·*没有中央管理机构等固定基础设施* Ad hoc 网络不依赖接入点、专用路由器以及传输线缆等设备,也没有集中的管理设施。在方便部署的同时,也带来了一些安全和管理的问题。

·*动态拓扑结构* 节点的任意、随机移动,加入或者退出,以及双向或者单向信道的区别,使得 Ad hoc 网络拓扑呈现随机动态变化和不可预测特性。

·*节点能量供应受限* 移动节点一般依赖于电池等可耗尽能源供电,可供使用的能量有限。这就导致在 Ad hoc 网络的设计和运作过程中,必须考虑如何以更有效的方式来使用有限能量。

·*节点的物理安全有限* 在战场等敌对环境中,移动节点可能被俘获、修改;在商业领域,移动节点也可能被盗窃或者恶意修改。这就给 Ad hoc 网络的安全问题带来极大的挑战。

由于 Ad hoc 网络能够快速而方便地部署,具有良好的分布性、独立性以及鲁棒性,因而在许多领域中可以得到广泛的应用。比如在军事通信领域,可用来构造战术互联网络,实现班组、装甲车辆以及机群之间的通讯,或用于已有军用网络的备用网络以提高军用网络的可靠性和生存性;在发生自然灾害,原有通信基础设施遭到破坏时,Ad hoc 网络可以快速组建网络恢复灾区通信,大大有利于救援实施;同时在商业、教育、会议、机场等民用领域,Ad hoc 网络也将得到广泛的应用。

3 Ad Hoc 网络路由协议

当两个节点不能直接通信时,需要其他中间节点进行数据转发。如何选择中间节点,即如何选择从源节点通往目的节点的路径,成为首先必须解决的问题。在传统网络里,由路由协议完成路径的建立。但是由于带宽和能量约束以及动态拓扑的原因,传统的路由协议并不能很好地适应 Ad hoc 网络环境。因此,设计适应 Ad hoc 网络特点的路由协议成为了研究的热点问题。由于单播通信在 Ad hoc 网络中应用最广,这里我们主要讨论单播路由协议。

Ad hoc 网络中的单播路由协议主要分为两大类。一类是基于拓扑信息的路由协议,可以进一步细分为先应式(proactive)路由协议和反应式(reactive)路由协议以及结合前两种协议优点的混合(hybrid)路由协议;另一类则是基于节点地理位置信息的路由协议[36]。

3.1 基于拓扑信息的路由协议

这类协议与传统的链路状态路由协议(LS)和距离矢量

路由协议(DV)一样,采用网络拓扑信息作为路由建立的基础,主要根据路由表和目的地址作转发决策。根据路由表建立方式的不同,基于拓扑信息的路由协议可以分为以下三类:

3.1.1 *先应式路由协议* 先应式路由协议又叫主动式,表驱动(table driven)路由协议。与传统LS或DV路由协议类似,这类协议通过周期性的交换网络拓扑更新信息,在每个节点构建当前网络拓扑结构视图。当需要向某个节点发送数据时,能从事先建立的路由表中快速查找到一条可用路径。然而,由于Ad hoc网络拓扑的动态变化导致周期性的拓扑更新信息要消耗大量的网络带宽,而Ad hoc网络中的有效带宽本来就很有限。因此,在如何减少拓扑更新信息对网络带宽的消耗方面,主动式路由协议要尽可能地优化。

主动式路由协议主要包括DSDV[5]、OLSR[27]、FSR[21]以及TBRPF[25]等路由协议。DSDV路由协议是最早提出的主动式路由协议,但是由于它的路由控制信息的开销太大,现在已经逐渐被抛弃。OLSR是针对Ad hoc网络特点进行了优化的链路状态路由协议,它的优化措施具体体现在:(1)采用MPR[1]广播算法有效减少拓扑更新信息的广播数量;(2)减小广播包的大小;从而有效降低路由控制信息对网络带宽的消耗。FSR路由协议根据节点间的距离(hop数)将网络划分为内部区域和外部区域;对不同区域内的节点的拓扑更新信息的广播频率不一样。关于内部区域链路状态信息的更新频率较高,以获得较精确的拓扑视图;对外部区域的链路状态信息更新频率较低,以降低对带宽的压力。

3.1.2 *反应式路由协议* 反应式路由协议又叫被动式,按需驱动(on-demand)路由协议。由于先应式路由协议的路由控制信息需要消耗大量的网络带宽,因此反应式路由协议采用了按需建立路由的方法。反应式路由协议一般包括两个过程:路径发现和路径维护。当源节点需要向某个目的节点发送信息时,如果路由表中没有可用路径时,将发起一个路由发现过程,通过路由请求信息和路由应答信息建立通往目的节点的路径。在数据发送过程中,还要利用路径维护来检测当前路径中是否发生路径中断(比如由于节点移动而导致),以维持路径的可用性。

DSR[8]和AODV[7]路由协议是反应式路由协议最典型的代表。顾名思义,DSR采用源路由,在路由发现阶段通过在网络中广播路由请求(RREQ),由目的节点或者其他中间节点返回路由应答(RREP),从而建立通往目的节点的路径。后续的数据发送在每个数据包头中包含了在路由发现阶段所建立路径所经过节点的完全列表。当路径中的某个节点检测到通往其下一跳的连接中断时,将向路径源节点返回路径错误(RERR)信息,通知源节点路径错误。DSR还采用路由缓冲措施来优化协议性能。AODV是传统DV协议的路径按需建立改进。在路由发现阶段仍然采用RREQ广播和RREP应答方式,在中间节点的路由表中建立通往目的节点的表项。AODV通过邻居节点之间交换的HELLO信息判断路径下一跳是否可达。节点向逐跳的上一跳邻居发送RERR消息通知连接失败,直到源节点得到这个通知消息。源节点这时可以再次发起路由发现过程以寻找另一条可用路径。AODV协议还采用序列号避免形成路径环路。

3.1.3 *混合路由协议* 先应式路由协议的路由控制信息网络带宽消耗较大,但是能够及时提供可用路径,减少路径发现过程导致的延迟;反应式路由协议解决了动态拓扑导致的频繁拓扑更新广播导致的带宽消耗,但是引入了路径发现延迟。混合路由协议试图将这两种协议的优点结合起来。目前提出的混合路由协议以ZRP[33]协议为代表。对网络中的每个节点,ZRP将距离该节点n跳范围内的节点划分为一个区域;在每个区域内部采用主动式路由协议IARP[34]交换路由信息,将路由广播控制在局部范围内;当目的节点不在源节点的同一个区域时,采用反应式路由协议IERP[35]进行路径发现。

3.2 基于位置信息的路由协议

这类路由协议主要依赖于节点定位服务(location service)和目的节点的位置信息作数据转发决策。随着户外和户内定位技术的发展和应用,基于位置信息的路由协议在技术上和经济上都是可行的。

LAR[28]路由协议是一种典型的基于位置信息的按需路由协议。LAR协议主要的贡献在于利用节点的位置信息,修改了反应式路由协议路由发现过程的广播方式,提高反应式路由协议的性能。它根据最近获得的目的节点的位置信息、移动速度以及时间间隔建立目的节点当前所在的期望域(expected zone),再根据特定的算法由期望域建立请求域(request zone)。LAR将源节点的路由发现请求包的传播限制所构建的请求区域内,从而减少了路由控制信息的开销。

基于位置信息的路由协议需要知道节点自己位置信息以及邻居节点和目的节点的位置信息。节点自身位置信息可以通过GPS定位设备取得;邻居节点的位置信息可以通过邻居间交换的HELLO信息获得;如何获取目的节点的位置信息则需要借助于定位服务(location service)。目前提出的定位服务包括DREAM[26]以及Grid[17]系统等。

4 路由协议面临的攻击和威胁

当前的路由协议没有考虑开放环境中潜在的安全问题,容易受到多种攻击,从而导致网络性能下降甚至整个网络的瘫痪。根据Ad hoc网络的部署方式和安全需求的不同,可以将Ad hoc网络的应用环境分为完全开放(open)、可管理开放(managed open)以及可管理敌对(managed hostile)三种[3],他们对安全性的需求依次增强。

4.1 完全开放Ad hoc网络的路由安全问题

在这种网络环境中,网络节点考虑更多的是如何以尽可能少的代价从网络中获取尽可能多的收益,从而表现出"自私"(selfishness)特性,导致网络连通性和性能下降。Ad hoc网络的基本运行方式是利用中间节点转发(forward)那些不能直接通信的节点之间的数据,而节点参与数据转发会使自己在某些方面蒙受损失:

·*能量消耗* 移动节点的能量供应一般是有限的,而数据转发却需要消耗较多的能量,可能导致节点能量过早耗尽,减少节点生存时间,或者节点用于自身通信的能量得不到满足。

·*自身数据发送延迟* 无线通信的可利用带宽相对较小,作为中间节点转发其他节点的数据,需要消耗一定的带宽,导致节点自身发送数据遭受更大的延迟。同时,数据转发也可能导致局部介质访问冲突,导致更大的冲突避让延迟。

因此,在完全开放的Ad hoc网络环境中,并不是每个节点都愿意无偿、主动的参与中间数据转发。同人类社会生活类似,移动节点会表现出"自私"特性。这种自私特性,主要体现在路由协议的数据转发阶段。这种拒绝转发数据的自私行为,实际上是一种针对路由协议的"拒绝服务(DoS)"攻击。文[4]指出了目前路由协议对节点自私性的忽略将会导致的问题,

并用仿真实验数据给出了这种攻击行为给网络性能带来的影响。

4.2 可管理 Ad hoc 网络的路由安全问题

与纯开放式 Ad hoc 网络中以节省资源(能量和带宽)为目的的自私行为相比,这种网络环境更多的是面临恶意攻击。根据攻击者是否参与路由协议过程,可以将攻击行为分为被动攻击和主动攻击[3]。

4.2.1 *被动攻击* 被动攻击并不对路由协议的操作进行任何形式的干扰,主要是通过监听无线通信的方式,获取路由信息包中的有价值信息。在敌对环境中,对路由信息包的监听和分析,可能得到网络中节点间的相互拓扑关系;在基于位置信息的路由协议中还可能得到节点具体的位置坐标信息,为下一步的打击提供依据。这种攻击方式难于被发现,但是如何从大量的路由信息中发现有价值的信息,对攻击者的分析、计算能力也是一个挑战。

4.2.2 *主动攻击* 主动攻击主要包括修改路由信息、假冒其他用户以及伪造路由信息、路由表溢出攻击等方式。

①修改路由控制信息 修改路由控制信息攻击主要手段是修改路径序列号、修改路径长度以及修改源路由列表。

·修改路径序列号。AODV 和 DSDV 等路由协议依赖于目的节点的序列号来判断路由表中通往目的节点的路径的新旧程度。在 AODV 路由协议中,对一个路由请求包(RREQ)的有效应答(RREP)必须有比 RREQ 更大的目的序列号。当某个节点向上游节点转发了第一个有效 RREP 应答后,后续的 RREP 如果没有比第一个 RREP 更大的序列号,后续的 RREP 应答将被丢弃;反之,将使用序列号更大的路径更新路由表。在图1所示的拓扑结构中,带箭头的实线表示两个相邻节点是可以直接通信的邻居节点;带箭头的虚线表示节点间存在的一条多跳路径;虚线上带问号则表示该路径可能并不存在。如果恶意节点 M 收到 B 广播的 RREQ 后,立即向 B 恶意返回一个拥有较大序列号的 RREP 应答(尽管 M 可能并不存在这样的路径),将会使其他节点(比如 C)返回的正确的 RREP 应答在 B 点被丢弃,从而使 S 发送的数据全部被重定向到恶意节点 M。这样,M 就可以通过修改序列号将自己插入节点 S 数据发送路径中,拦截 S 发往 D 的数据,并进行分析、篡改或者丢弃。

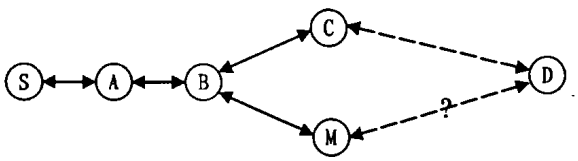

图1 修改序列号攻击

·修改路径长度。在 AODV 路由协议中,当源节点收到几个 RREP 应答有相同的序列号时,将使用距离最短(hop 数最少)的路径。这样,恶意节点可能向源节点声明自己到达目的节点的距离最近,比如只有1个 hop,从而使自己成为通信中间节点的机会大大增加。同样在图2中,恶意节点 M 尽管返回正常的序列号,但是宣称自己到目的节点的路径最短(实际上 M 到达 D 的路径可能距离最长)。这样,当两个路由请求应答同事到达 S 时,S 将会采用经过 M 的看起来更短的路径。

·修改源路由。DSR 路由协议使用源路由,在每个数据包头中包含了通往目的节点的完整路径(所经过的中间节点的全部列表)。由于目前的 DSR 协议没有引入安全措施确保源路由信息的完整性,恶意节点能够很容易地修改源路由从而发起 DoS 攻击。

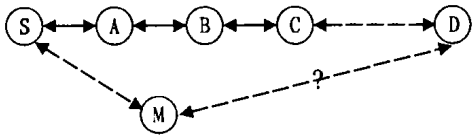

图2 修改路径长度攻击

考虑图3的网络拓扑。C、E 之间的虚线表示 C、E 之间不能直接通信,存在其他中间节点。假设源节点 S 有一条通往目的 D 的唯一路径 $S-A-M-C\cdots\cdots E-D$。当数据包到达恶意节点 M 时,M 可以将数据包头中的源路径列表修改,比如删去节点 E。由于 C、D 之间不能直接通信,这样数据包就不能到达目的节点 D。

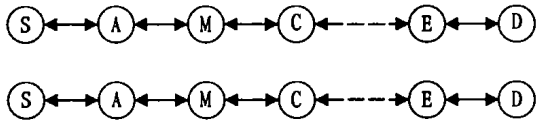

图3 修改源路由攻击

同样,恶意节点 M 也可以向源路由中插入其他恶意节点,比如 M',使源路径变成 $S-A-M-M'-C\cdots\cdots E-D$,并同 M' 合谋,使数据经过 M' 后再经过 C 到达目的节点 D。此外,DSR 还用路径错误包来维护路径。恶意节点 M 也可以通过丢弃 C 返回的路径错误包,阻止源节点了解路径故障,使源节点发出的数据在 C 处因为路径故障而丢弃。还有,DSR 虽然在路径发现阶段能够避免形成路径环路,凡是不能防止恶意节点通过修改源路径引入路径环路。

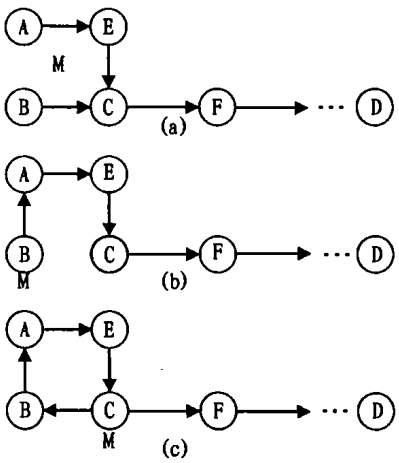

图4 假冒其他用户身份实施攻击

②假冒其他用户 在 Ad hoc 网络中常常采用 MAC 地址或者 IP 地址作为节点身份的标识。但这些标识很容易被修改,从而使攻击者可以假冒其他用户身份。以图4(a)、(b)、(c)所示攻击为例,恶意节点 M 通过假冒其他节点身份可以在网络中造成路径环路。假设经过 RREQ 和 RREP 交换后,已经建立了图示的路径。其中,A 处于 B、E 的发送范围;B 处于 A、C 的发送范围;E 处于 A、C 的发送范围,C 处于 B、E 和 F 的发送范围,而 F 处于 C 以及下一跳邻居的发送范围之内。M 通过对 RREQ 以及 RREP 信息的监听,可以发现这种拓扑关系。为了造成路径环路,M 首先通过修改自己的 MAC 地址假冒 A,然后移动到 B 附近,而且保证 A 不能接收到其发出的信息。然后 M 向 B 发出一个比前面 C 返回的 RREP 距离

更短的 RREP，从而使 B 通往目的节点的路径的下一跳设定为 $A(a)$。类似地，M 可以假冒节点 B，给 C 发送错误的 RREP 信息，使 C 将通往目的节点的路径的下一跳设定为 $B(b)$。这样，将在 A、B、C 和 E 之间形成路径环路(c)，使他们都不能和目的节点 D 通信。如果网络中同时存在多个这样的恶意节点，通过合谋，恶意节点将能够更容易地造成路径环路。

③伪造路由信息

·伪造路由错误(RERR)消息。AODV 以及 DSR 等反应式路由协议使用路径维护来保证路径的连通性。当某个节点发现路径中下一跳不可达(即发生了连接中断)时，将向路径的上游节点返回指示连接断裂的 RERR 信息。源节点收到错误报告后，将采取措施努力从错误中恢复，比如重新发起路径发现过程以寻找新的可用路径等。恶意节点可以通过伪造 RERR 消息破坏路径的可用性，发起 DoS 攻击。假定图5中存在一条 $S-A-B-C-E-D$ 的路径。恶意节点可以结合前面的假冒身份的方法，假冒 C 向 B 发送指示 C、E 之间路径中断的 *RERR* 错误报告。B 将删除其路由表内通往 E 的表项，并将该错误报告向上游邻居 A 转发。当错误报告到达 S 时，S 将重新发起一个路径发现过程试图建立一条新的通往 D 的路径。这样，M 就能通过伪造的路径错误消息破坏路径可达性，增加源节点的路径建立消耗，降低网络性能。

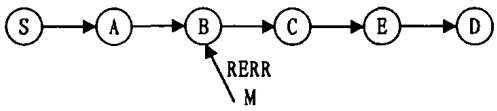

图5 伪造 RERR 信息攻击

·破坏 DSR 协议的路径缓冲。为了提高协议性能，DSR 路由协议引入了路径缓冲(route cache)的概念。节点除了从自己转发的数据包头中获取路径信息之外，还能从被动接收(监听)到的数据包头中获取路径信息，并将这个路径信息存入本地路径缓冲，以备将来使用。这样能够减少路径发现的开销，提高协议性能。但是也引入了新的安全脆弱性。恶意节点 M 可以通过向邻居广播通往某个节点的伪造路径信息，使其周围的邻居节点将这个路径信息存入路径缓存，形成错误路径。

·路由表溢出攻击。移动设备的内存本来就不充足，而用于路由表的空间则进一步有限。在 DSDV 等主动式路由协议中，网络节点要周期性的交换路由信息。恶意节点 M 可以通过伪造大量的虚假路由信息，这些路由信息通往实际不存在的目的节点，从而使其他网络节点的路由表空间被这些虚假的路由信息占用，甚至溢出，使得那些真实的路由信息被丢弃。对于反应式路由协议，两个或多个恶意节点之间通过合谋，也可以发起这种攻击。

④隧道(tunneling)攻击　也叫 wormhole 攻击，其基本方法是将数据在一个恶意节点处进行封装(encapsulation)，再通过一条已知路径发往另一个恶意节点，然后再解包，获取原数据，并将该数据从隧道的另一端注入网络。需要两个或更多的恶意节点通过合谋，才能发起隧道攻击。其效果就好像在两个恶意节点之间建立一条直接的路径，尽管实际上并不存在这样的物理路径。

在图6中，$M1$和 $M2$是两个恶意节点，粗实线代表真实的路径，细实线代表隧道，虚线代表恶意节点所声明的一条虚拟路径。以 AODV 协议为例，当 $M1$接收到 S 发出的 RREQ 时，$M1$将该 RREQ 以数据载荷(payload)的方式通过一条已知路径比如 $M1-A-B-C-M2$发往 $M2$。$M2$接收到该数据包以后，提取该 RREQ 信息，并将其转发给目的节点 D。这样在 D 看来，似乎存在一条 S 经过 $M1$和 $M2$的路径。当然，RREQ 信息仍然能够通过正确的路径 $S-A-B-C-D$ 到达目的节点。D 将向两条路径都返回 RREP 应答。如果 $M2$同样采用隧道的方式将该应答发送给 $M1$，就会使 S 错误地认为通过 $M1$ 的路径的距离较短，是一条更优的路径。这样，S 发出的数据就会在 A、B、C 的转发下，经过两个恶意节点。恶意节点可以选择丢弃或者修改源节点和目的节点之间交换的数据。

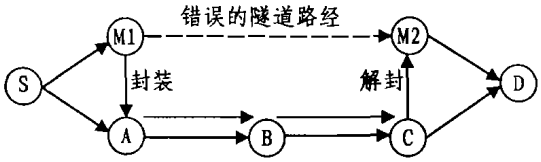

图6 隧道攻击

DSDV、OLSR 等主动式路由协议通过交换 HELLO 信息来发现邻居节点。两个合谋的恶意节点可以通过隧道攻击，使两个物理不相邻的节点误以为彼此是邻居。比如，恶意节点 $M1$将 A 的 HELLO 信息通过隧道原封不动的传给 $M2$，再由 $M2$广播给 C；$M2$再把 C 广播的 HELLO 包经 $M1$传给 A，使 A、C 误以为彼此能够直接通信。实际上，当 A 试图给 C 直接发送数据时，这些数据并不能到达 B。

这种隧道攻击对多径(multi-path)路由协议也是一个安全问题。多径路由的本质是要在源和目的之间寻找多条互不相交的路径。以图6所示拓扑为例，S 会错误地认为存在两条互不相交的路径 $S-M1-M2-D$ 和 $S-A-B-C-D$ 通往同一目的节点。事实上，两条看似独立的路径存在 A、B、C 三个公共中间节点。

4.2.3 Rushing 攻击[32]　反应式路由协议在路由发现阶段需要使用 RREQ 广播。为了减少这种广播对带宽的消耗，AODV、DSR 等路由协议规定，当一个节点收到多个属于同一个路径发现过程的 RREQ 包时，只转发最先收到的请求包，而将后续到达的请求包丢弃。如果某个恶意节点能够使目的节点所有的邻居节点最先收到的 RREQ 包都经过该恶意节点，就能使目的节点忽略通过其他正确路径达到的路由请求，从而使源节点和目的节点的通信都通过该恶意节点。如图7所示，两个阴影节点为目标节点 D 的邻居节点。如果恶意节点 M 能够将源自 S 的路由请求先于 C 和 E 发送到 D 的两个邻居节点。那么，可以保证 S 到 D 的路径必然经过 M。

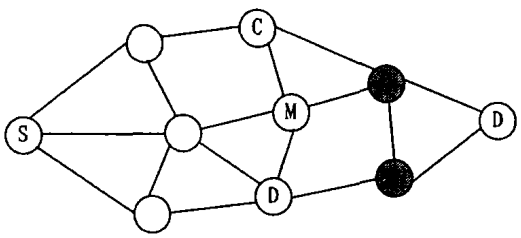

图7 Rushing 攻击

4.2.4 基于分簇的路由协议安全问题　除了平面式的网络组织结构外，为了弥补 Ad hoc 网络中因为缺少基础设施的不足，有人提出通过分簇(clustering)的方法在 Ad hoc 网络中构建虚拟骨干网络，提高网络性能和协议可扩展性(scal-

ability)。基于分簇的路由协议的一个核心问题就是簇首(cluster head)的选举。如果当前簇首由于移动等原因失效,需要重新选举簇首节点。由于簇首负责了本簇内节点与其他簇之间的全部数据转发和路由信息控制,因此如果恶意节点 M 通过假冒等方法,获取了簇首地位,恶意节点就能够丢弃本簇内其他节点的数据,形成不可达的网络孤岛。

5 可能的防护方法

针对纯开放式 Ad hoc 网络环境中节点的"自私"特性,Hubaux 等人提出了基于虚拟货币的协作数据转发激励机制[14~16]。其核心思想是通过引入虚拟货币,将数据转发作为一种有偿服务。源节点需要为数据发送支付货币,否则不能发送数据;中间节点从转发数据中获取报酬,以弥补转发数据所蒙受的损失。文[6,22]将整个网络视为一个各成员之间共享资源的社区。成员是否能够使用社区资源,取决于成员对社区的贡献和成员的声誉。通过在网络中引入某种检测方法,节点的自私行为将导致自身声誉的降低。如果这种可信任程度低于某个阈值,那么自私节点将被排除在网络之外,剥夺其使用网络资源的权利。

针对军事、应急响应等关键应用中的路由安全问题,主要的防范措施是使用加密方法确保路由信息的完整性和真实性,防止路由信息被恶意修改,防止恶意节点产生伪造的路由信息。主要的研究成果包括:SEAD[31]、SRP[23]、ARAN[3]、ARIADNE[30]、SAODV[2]等安全路由协议。文[29]还针对基于位置信息的路由协议提出了旨在保护节点位置信息机密性的安全路由协议。

由于 Ad hoc 网络是一个完全分布的计算环境,而且每个节点的计算资源和能量、带宽资源有限。使用基于数据加密方法的安全防护,其核心问题是如何在 Ad hoc 网络这样一个特殊的场景下实现鲁棒的、可扩展的、高效的密钥管理机制。文[9~13,18,19]讨论了 Ad hoc 网络中的密钥管理问题。

此外,在比如战场等敌对环境下,移动节点的物理安全得不到保证。合法节点可能被俘获,从而使攻击者可能掌握安全密钥。有人提出将 Internet 中的入侵检测技术(IDS)用来在 Ad hoc 网络中检测这种取得了合法身份的恶意攻击[20]。然而,由于 Ad hoc 网络的特殊性,目前的 IDS 技术还不能很好地适用其中。

结束语 自组织的 Ad hoc 网络改变了传统网路的概念,是一种全新的通信手段。安全保障是 Ad hoc 网络得以广泛部署的前提。路由协议的安全则是整个网络安全的基础。本文对 Ad hoc 网络路由协议可能面临的攻击进行了分析,重点描述了攻击过程,为设计、实现安全路由提供了有益的帮助。

同时,Ad hoc 网络与具体的应用密切相关,不同的应用环境对安全性的要求不一致,没有任何安全措施能够解决不同应用环境下所产生的全部安全问题。因此,在设计安全路由协议时应该充分结合具体的应用,根据具体的环境实施具体的安全保护。

参 考 文 献

1 Qayyum A, Laouiti A, Viennot L. Multipoint Relaying: An Efficient Technique for Flooding in Mobile Wireless Networks. In: Proc. of 35th Annual Hawaii Intl. Conf. on System Sciences (HICSS'2001), 2001

2 Zapata M G, Asokan N. Securing Ad Hoc Routing Protocols. In: Proc. of ACM WiSe'02, Atlanta, Geogia, USA, Sep. 2002

3 Dahill B, et al. A Secure Routing Protocol for Ad Hoc Networks. In: Proc. of the 10th IEEE Intl. Conf. on Network Protocols (ICNP), Nov. 2002

4 Lamparter B, Plaggemeier M, Westhoff D. Analysis of Co-operation Approaches in Ad Hoc Networks. In: Proc. of WiOpt'03, INRIA Sophia-Antipolis, France, March, 2003

5 Perkins C E, Bhagwat P. Highly Dynamic Destination-Sequenced Distance Vector (DSDV) for Mobile Computers. In: Proc. of the SIGCOMM 1994 Conf. on Communications Architectures, Protocols and Applications, Aug. 1994

6 Buchegger S, Boudec J L. Performance Analysis of the CONFIDANT Protocol. In: Proc. of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHoc), EPFL Lausanne, Switzerland, June 2002

7 Perkins C E, Royer E M B, Das S R. Ad hoc On-Demand Distance Vector (AODV) Routing. draft-ietf-manet-aodv-11. txt. June 2002. (expired)

8 Johnson D B, et al. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR). draft-ietf-manet-dsr-07. txt. Feb. 2002. (expired)

9 Fokine K. Key Management in Ad Hoc Networks: [Technical Report. LITH-ISY-EX-3322-2002]. Sep. 2002

10 Asokan N, Ginzboorg P. Key Management in Ad Hoc Networks. ComputerCommunications, 2000, 23

11 Giordno S. Mobile Ad-Hoc Networks. Addison-Wesley, 2000

12 Luo H, Kong J, Zerfos P, Lu S, Zhang L. Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks. In: Proc. of IEEE ICNP, 2001

13 Zhou L, Hass Z J. Securing Ad Hoc Networks. IEEE Networks Special Issue on Network Security, 1999, 13 (6): 24~30

14 Buttyan L, Hubaux J P. Enforcing Service Availability in Mobile Ad-hoc WANS. In: Proc. of 1st IEEE/ACM Workshop on Mobile Ad hoc Networking and Computing (MobiHoc 2000), Lausanne, Switzerland, 2000

15 Buttyan L, Hubaux J P. Nuglets: a Virtual Currency to Stimulate Cooperation in Self-Organized Ad hoc Networks: [Technical Report. EPFL-DSC-ICA, CH-1015]. Swiss Federal Institute of Technology. Lausanne. Jan. 200

16 Buttyan L, Hubaux J P. Stimulating Cooperation in Self-organized Mobile Ad Hoc Networks. ACM Journal for Mobile Networks (MONET), special issue on Mobile Ad Hoc Networks. 2002

17 Li J, et al. A Scalable Location Service for Geographic Ad Hoc Routing. In: Proc. of ACM/IEEE MobiCom'00, Bostan, MA, USA, 2000

18 Yi S, Kravets R. Key Management for Heterogeneous Ad Hoc Wireless Networks: [Technical Report. UIUCDCS-R-2002-2290]. University of Illinois at Urbana-Champaign. July, 2002

19 Buttyan L, Hubaux J P, Capkun S. The Quest for Security in Mobile Ad Hoc Networks. In: Proc. of ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), Long Beach, CA, 2001

20 Zhang Y, Lee W. Intrusion Detection in Wireless Ad-Hoc Networks. In: Proc. of the sixth Annual Intl. Conf. on Mobile Computing and Networking (MobiCom'00), Boston, Masachussetts, USA, Aug. 2000

21 Gerla M, Pei G, Hong X Y, Chen T-W. Fisheye State Routing Protocol (FSR) for Ad Hoc Networks. draft-ietf-manet-fsr-00. txt. June 2001. (work in progress)

22 Michiardi P, Molva R. Core: A COllaborative REputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks. In: Proc. of the sixth IFIP Conf. on Security Communications and Multimedia (CMS 2002), 2002

23 Papadimitrators P, Hass Z J, Zhou L. Secure Routing for Mobile Ad hoc Networks (SRP). In: Proc. of SCS Communication Networks and Distribute System modeling and Simulation Conf. (CNDS), San Antonio, TX, 27-1, 2002

24 Perkins C E. Ad Hoc Networking. Addison-Wesley, Boston, 2001. ISBN 0201309769

25 Ogier R G, Templi F L, Bellur B, Lewis M G. Topology Broadcast Based on Reverse-Path Forwarding (TBRPF). draft-ietf-manet-tbrpf-05. txt. March 2002. (expired)

26 Basagni S, Chlamtac I, Syrotiuk V R, Woodward B A. A Distance Routing Effect Algorithm for Mobility (DREAM). In: Proc. of

ACM/IEEE Mobicom'98,Oct. 1998
27 Clauser T,Jacquet P,Laouiti A,et al. Optimized Link State Routing Protocols. draft-ietf-manet-olsr-04. txt. June 2001. (work in progress)
28 Ko Y-B,Vaidya N H. Location-Aided Routing (LAR) in Mobile Ad Hoc Networks. In:Proc. of ACM/IEEE MOBICOM'98,Oct. 1998
29 Carter S,Yasinsac A. Secure Position Aided Ad hoc Routing Protocol. In:Proc. of the IASTED Intl. Conf. on Communications and Computer Networks (CCN02),Nov. 2002
30 Hu Y-C,Perrig A,Johnson D B. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. In:Proc. of the 8th ACM Intl. Conf. on Mobile Computing and Networking (MobiCom), September,2002
31 Hu Y-C,Johnson D B,Perrig A. SEAD:Secure Efficient Distance Vector Routing for Mobile Ad Hoc Networks. In:Proc. of the 4th IEEE Workshop on Mobile Computing System and Application (WMCSA),June,2002
32 Hu Y-C,Perrig A,Johnson D B. Rushing attacks and defense in wireless Ad hoc network routing protocols. In:Proc. of the 2003 ACM workshop on Wireless security (WiSe'03),San Diego,CA,USA,2003
33 Hass Z J,Pealman M R,Samar P. The Zone Routing Protocol (ZRP) for Ad Hoc Networks. draft-ietf-manet-zrp-04. txt. July 2002. (workin in progress)
34 Hass Z J,Pealman M R,Samar P. The IntraZone Routing Protocols (IARP) for Ad Hoc Networks. draft-ietf- manet-zone-iarp-02. txt. July 2002. (work in progress)
35 Hass Z J,Pealman M R,Samar P. The InterZone Routing Protocol (IERP) for Ad Hoc Networks. draft-ietf-manet-zone-ierp-02. txt. July 2002. (work in progress)
36 Zhou H. A Survey on Routing Protocols in MANETs:[Technical Report. MSU-CSE-03-08]. Department of CSE in Michigan State University. Mar. 2003

(上接第35页)

动设备端的 J2ME 程序通过 HTTP 协议经由无线网络同中间层进行交互以实现应用过程。

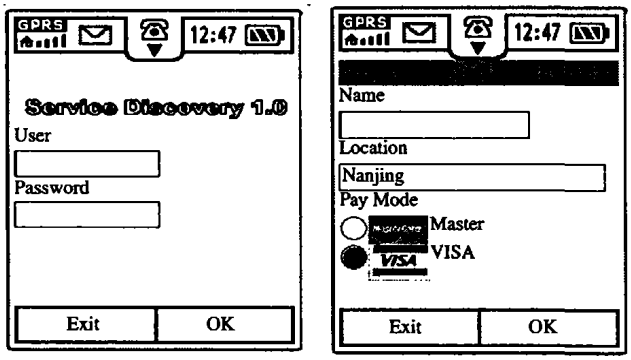

图6 用户 Agent 运行界面

根据系统的应用流程,我们设计了登录,服务请求,表单报告以及结果查询等四组协议。通过交互协议规范了服务发现系统中各模块之间的数据流动。

服务发现代理 Agent 是整个发现过程的中枢部件,它通过和无线消息服务器的交互得到移动用户的有关指令,并同系统中其它部件如服务 Agent 交互,负责组织服务的发现。本系统中,代理 Agent 驻扎在消息服务器上,所以和消息服务器的交互比较方便实现。

我们在此基础上设计了一个发现购书服务的模拟实例,用户可以随时随地通过手机端登录到系统去查询获取购买图书的服务。

我们通过这个实例验证了基于 Agent 的移动应用框架的可行性,并得到了一些和移动应用系统的设计、部署相关的实践经验,为进一步研究奠定了基础。

结论和展望 在本文中,我们仔细分析了无线网络和移动设备的特点,提出了基于 Agent 的移动应用框架的设计方案,并在一个服务发现系统中应用了这个框架设计思想。

无线网络和移动计算设备等相关技术正在不断的发展,关于移动计算领域的研究也越来越多,我们将结合已有工作在以下几个方面作进一步的研究:

1)我们将进一步拓展移动应用的场景。任何一个研究都不能脱离应用,我们拟在移动银行、移动商务等领域部署实现该框架,在应用中我们肯定还会发现一些新的问题,得到一些新的启示,将会对移动系统的框架作改进和补充。

2)移动中间件方面的研究。从本文可以看出,移动应用系统的中间层是非常重要的,我们将尝试把一些新型技术如移动 Agent 技术、MOM 技术等运用到移动应用系统的中间层中,使得移动中间件在面向移动用户的系统中更好地发挥作用。

3)移动应用的安全研究。随着移动应用的日益广泛,移动系统的安全性要求越来越高,而目前,无论在底层无线网络,还是在其上面的移动应用系统,安全性能都还很薄弱,我们将把研究的重点放在后者,将安全特性加到我们的设计框架中来。

参 考 文 献

1 Duchamp D. Issues in Wireless Mobile Computing IEEE Computer Society Press,1992. 2～10
2 Gte J,Helal A. Client-Server Computing in Mobile Environments. ACM Computing Surveys,1999,31(2)
3 Eisenstein J,Vanderdoncki J,Puerta A. Adapting to Mobile Contexts with User-Interface Modeling. In:the 3rd IEEE Workshop on Mobile Computing Systems and Applications,Dec. 2000. 83～92
4 Mascolo C,Capra L,Zachariadis S,Emmerich W. A Data-Sharing Middleware for Mobile Computing Int. Journal on Personal and Wireless Communications
5 Abowd G,Atkeson C,Hong J,et al. A mobile context-aware tour guide ACM Wireless Networks,1997,3:421～433
6 陶先平,吕建,马晓星,胡昊. 移动 Agent 系统基准模型的研究. 电子学报,2002,12:2019～2021
7 陶先平,吕建,张冠群,李新. 一种新的移动 agent 结构化迁移机制的设计和实现. 软件学报,2000,11(7):918～923
8 Feng Xinyu,Cao Jiannong,Lü Jian, Chan H. An Efficient Mailbox-Based Algorithm for Message Delivery in Mobile Agent Systems,Lecture Notes in computer science,2001,2240: 135～151
9 李新,吕建,张冠群,冯新宇,曹春,陶先平. 移动 Agent 的安全性研究. 软件学报,2002,13(10):1991～2000
10 XML 1.0 Recommendation. http://www.w3.org/TR/2000/REC-xml-20001006
11 W3C, Document Object Model (DOM) Level 1 Specification. http://www.w3.org/TR/REC-DOM-Level-1/
12 Sun Microsystems. Java 2 Platform Micro Edition (J2ME) Technology for Creating Mobile Devices,White Paper,May 2000
13 Sun Microsystems. Jini Architecture Specification. http://www.sun.com/software/jinni /specs/
14 Sun Microsystems. Midp Specification. http://java.sun.com/products/midp/